PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-276457
(43)Date of publication of application : 06.10.2000

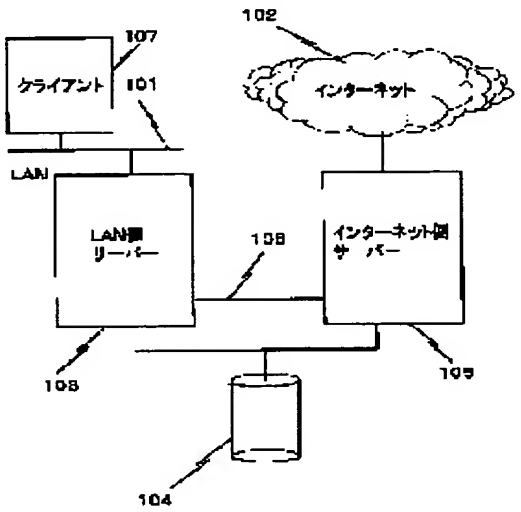
(51)Int.Cl. G06F 15/177
G06F 13/00
H04L 12/54
H04L 12/58

(21)Application number : 11-081049
(22)Date of filing : 25.03.1999

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : SAKAKURA TAKASHI

(54) DATA SHARING COMPUTER SYSTEM AND CLIENT

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a service copy server which safely shares data between different networks like an intra-enterprise network and the Internet and which copies services for each network.
SOLUTION: A LAN-side server 103 connected to a LAN 101 and an Initernet-side server 105 connected to the Internet 102 share data on a shared disk 104 for which they use a bus 106 with a bus lock function to exclusively control, and they use this data to provide the same services respectively.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２０００－２７６４５７
（Ｐ２０００－２７６４５７Ａ）
(43)公開日　平成12年10月6日(2000.10.6)

(51)Int.Cl.[7]		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/177	６８２	Ｇ０６Ｆ	15/177	６８２Ｆ	5B045
	13/00	３５１		13/00	３５１Ｚ	5B089
Ｈ０４Ｌ	12/54		Ｈ０４Ｌ	11/20	１０１Ａ	5K030
	12/58					

審査請求　未請求　請求項の数１１　ＯＬ　（全２６頁）

(21)出願番号　特願平11-81049

(22)出願日　平成11年3月25日(1999.3.25)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目2番3号

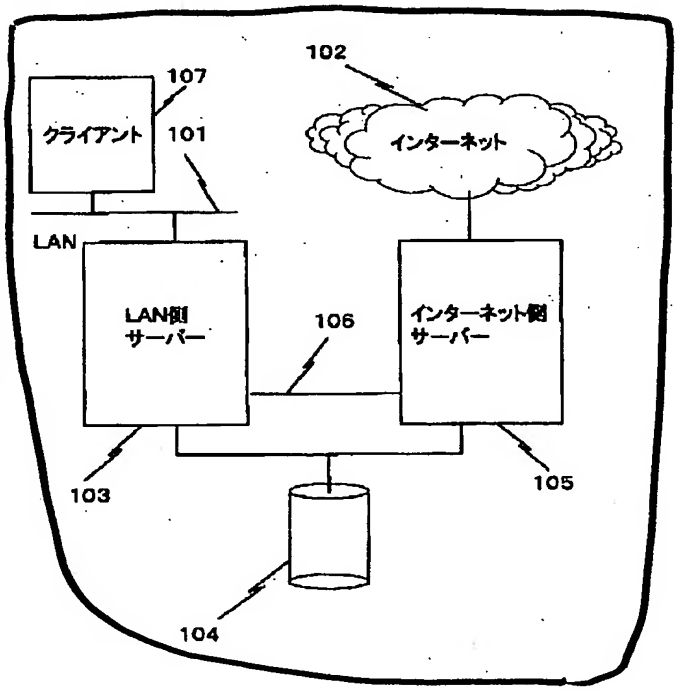
(72)発明者　坂倉　隆史
東京都千代田区丸の内二丁目2番3号　三菱電機株式会　社内

(74)代理人　100102439
弁理士　宮田　金雄　（外2名）

Ｆターム(参考)　5B045 BB12 EE06 GG01 JJ33
5B089 GA11 GA19 GA21 HA06 HA08
HA10 KA00 KA17 KB13 KC28
KC57 KC58 KD02 KH30
5K030 GA15 HC01 HC13 HD06 KA02

(54)【発明の名称】データ共有コンピュータシステム及びクライアント

(57)【要約】
【課題】　企業内ネットワークとインターネットのように異なるネットワーク間で安全にデータを共有し、ネットワーク毎にサービスを複製するサービス複製サーバーを提供する。
【解決手段】　ＬＡＮ１０１に接続されたＬＡＮ側サーバー１０３と、インターネット１０２に接続されたインターネット側サーバー１０５とが、バスロック機能付きバス１０６を用いて排他制御する共有ディスク１０４上でデータを共有し、そのデータを用いて、それぞれに同一のサービスを提供することを特徴とする。



【特許請求の範囲】

【請求項１】　第一のコンピュータシステムと、第二のコンピュータシステムと、共有データ記憶部と、アクセス可否情報記憶部とを備えるデータ共有コンピュータシステムであって、（Ａ）共有データ記憶部は、複数のデータ記憶領域を有し、第一のコンピュータシステム及び第二のコンピュータシステムからアクセスされる共有データを、複数のデータ記憶領域に分割して記憶し、

（Ｂ）アクセス可否情報記憶部は、共有データ記憶部の各データ記憶領域に対応して、そのデータ記憶領域に対してアクセス可能あるいはアクセス不可であることを意味するアクセス可否情報を記憶し、（Ｃ）第一のコンピュータシステムは、第一のサービス部と、共有データ記憶部に接続する第一のデータアクセス部と、アクセス可否情報記憶部に接続する第一の排他制御部とを備え、

（１）第一のサービス部は、第一のデータアクセス部と第一の排他制御部に対して、任意のデータ記憶領域に対するアクセスを指示し、

（２）第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更し、

（３）第一のデータアクセス部は、第一の排他制御部により、アクセス可能と判定され、アクセス可否情報をアクセス不可に変更された後に、指示されたデータ記憶領域にアクセスし、

（４）第一の排他制御部は、第一のデータアクセス部により、指示されたデータ記憶領域に対してアクセスされた後に、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更し、（Ｄ）第二のコンピュータシステムは、第二のサービス部と、共有データ記憶部に接続する第二のデータアクセス部と、アクセス可否情報記憶部に接続する第二の排他制御部とを備え、

（１）第二のサービス部は、第二のデータアクセス部と第二の排他制御部に対して、任意のデータ記憶領域に対するアクセスを指示し、

（２）第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更し、

（３）第二のデータアクセス部は、第二の排他制御部により、アクセス可能と判定され、アクセス可否情報をアクセス不可に変更された後に、指示されたデータ記憶領域にアクセスし、

（４）第二の排他制御部は、第二のデータアクセス部により、指示されたデータ記憶領域に対してアクセスされた後に、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更することを特徴とするデータ共有コンピュータシステム。

【請求項２】　第一のコンピュータシステムは、第三のコンピュータシステムを有する第一のネットワークシステムに接続し、

第一のサービス部は、第一のネットワークシステムを介して第三のコンピュータシステムに対してサービスを提供し、

第二のコンピュータシステムは、第四のコンピュータシステムを有する第二のネットワークシステムに接続し、

第二のサービス部は、第二のネットワークシステムを介して第四のコンピュータシステムに対してサービスを提供することを特徴とする請求項１記載のデータ共有コンピュータシステム。

【請求項３】　第二のサービス部は、第一のサービス部が第一のネットワークシステムを介して第三のコンピュータシステムに対して提供するサービスと等価のサービスを、第二のネットワークシステムを介して第四のコンピュータシステムに対して提供することを特徴とする請求項２記載のデータ共有コンピュータシステム。

【請求項４】　第一の排他制御部は、バスロック機能付きバスによって、アクセス可否情報記憶部に接続し、

第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する間、バスをロックし、

第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更する間、バスをロックし、

第二の排他制御部は、上記バスロック機能付きバスによって、アクセス可否情報記憶部に接続し、

第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する間、バスをロックし、

第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更する間、バスをロックすることを特徴とする請求項１記載のデータ共有コンピュータシステム。

【請求項５】　第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する一連の動作を、一の命令で実行し、

第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶

領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する一連の動作を、一の命令で実行すること特徴とする請求項１記載のデータ共有コンピュータシステム。

【請求項６】　第一のコンピュータシステムは、以下の要素を備えることを特徴とする請求項１記載のデータ共有コンピュータシステム

（１）データの暗号化及び復号化に用いる暗号鍵を記憶する暗号鍵記憶部、（２）暗号鍵を指定して暗号化を指示された場合には、指定された暗号鍵を用いてデータを暗号化し、暗号鍵を指定して復号化を指示された場合には、指定された暗号鍵を用いてデータを復号化するデータ暗号化／復号化実行部、（３）暗号鍵記憶部が記憶する暗号鍵を変更する暗号鍵再設定部、（４）第一のデータアクセス部に、データ記憶領域からの暗号データの読み出しを指示し、

データ暗号化／復号化実行部に、変更前の暗号鍵を指定して、読み出した暗号データの復号化を指示し、

データ暗号化／復号化実行部に、変更後の暗号鍵を指定して、復号化したデータの再暗号化を指示し、

第一のデータアクセス部に、再暗号化したデータを、元のデータ記憶領域へ書き込むことを指示するデータ再暗号化部。

【請求項７】　ネットワークシステムに接続するクライアントであって、以下の要素を有するクライアント

（１）上記ネットワークシステムに接続する第一のコンピュータシステムであって、第二のコンピュータシステムとデータを共有する第一のコンピュータシステムに対して、共有データを送信し、また、共有データを受信する共有データ送信／受信部、（２）データ送信／受信部が送信する共有データを暗号化するデータ暗号化部、

（３）データ送信／受信部が受信した共有データを復号化するデータ復号化部。

【請求項８】　データ共有コンピュータシステムは、第三のコンピュータシステムを有し、

第三のコンピュータシステムは、第一のコンピュータシステムが接続する第一のネットワークシステムに接続し、

第一のサービス部は、第一のネットワークシステムを介して第三のコンピュータシステムに対してサービスを提供し、

第三のコンピュータシステムは、第一のサービス部が提供するサービスによってアクセスした共有データをキャッシュする共有データキャッシュ部を有することを特徴とする請求項１記載のデータ共有コンピュータシステム。

【請求項９】　第一のサービス部は、第一の構成情報を用いて動作し、

共有データ記憶部は、第一のサービス部が用いる第一の構成情報を記憶し、

第二のコンピュータシステムは、他の記憶部を有し、

第二のコンピュータシステムは、共有データ記憶部に記憶されている第一の構成情報を読み出し、読み込んだ第一の構成情報を他の記憶部に書き込む構成情報複製部を有し、

第二のサービス部は、他の記憶部に書き込んだ第一の構成情報を更新し、更新した第二の構成情報を用いて動作することを特徴とする請求項１記載のデータ共有コンピュータシステム。

【請求項１０】　第一のコンピュータシステムは、以下の要素を備えることを特徴とする請求項１記載のデータ共有コンピュータシステム

（１）第一のコンピュータシステムによるユーザ認証の認証方式を記憶する認証方式管理部と、（２）認証に用いるデータを予め記憶する認証データベース管理部と、

（３）認証要求と認証を受ける為のデータとを受付け、認証を受ける為のデータと、認証データベース管理部に予め記憶された認証に用いるデータとを用いて、認証方式管理部に記憶された認証方式により、ユーザ認証を行なう認証機能部。

【請求項１１】　データ共有コンピュータシステムは、バスを備え、第一のコンピュータシステムと、第二のコンピュータシステムと、共有データ記憶部と、アクセス可否情報記憶部とが上記バスに接続された共有メモリ型並列計算機であることを特徴とする請求項１記載のデータ共有コンピュータシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、第三者がアクセスし、利用するインターネットなどのネットワーク上で、安全にデータ提供サービスを行なうサーバー装置に係り、第三者のアクセスから保護すべきネットワークとデータを共有するサーバー装置に関する。

【０００２】

【従来の技術】近年インターネット利用が普及し、ＷＷＷ（Ｗｏｒｌｄ－Ｗｉｄｅ　Ｗｅｂ）、電子メールなどのインターネットを利用したアプリケーションの利用がごく一般的に行なわれるようになってきた。これらのアプリケーションによって、インターネットを利用して、企業や、教育機関などが提供する情報を参照することや、通信目的の利用が可能になった。

【０００３】しかし、インターネットに接続することは、インターネット上に接続されたいずれのサイトにも自由にアクセスできるという利便性をもたらす一方、悪意の第三者からの攻撃に晒されるという危険性をもたらすことを意味する。

【０００４】そこで、一般に企業では、企業内のネットワークシステムをインターネット接続する必要がある場合、インターネットへの接続箇所を限定し、その個所に

ファイアウォールと呼ばれる、特定の通信のみその通過を許す機構を設け、そのファイアウォールを介して接続することにより、企業内のネットワークをインターネット経由の第三者からの攻撃から保護する運用がなされてきた。そして、一般に企業内ネットワークの安全性がインターネット接続の利便性より重視されるため、ファイアウォールの構成としては、ごく限られた通信、例えば、電子メールの送信プロトコルである　ＳＭＴＰ（ｓｉｍｐｌｅ　ｍａｉｌ　ｔｒａｎｓｆｅｒｐｒｏｔｏｃｏｌ）メッセージのみが通過できるというものが多い。

【０００５】これに対して、特開平９－２７０７８８には、ファイアウォールの運用において、インターネット接続の利便性と安全性を両立させるために、通信パケットにファイアウォールからの認証チャレンジに応答するプログラム機能を持たせ、特定の認証ポートを通して通信できるようにすることにより、ファイアウォールの構成を変えなくてもインターネットからの種々のサービス要求に対応できる技術が開示されている。これにより、企業内のネットワークの安全を保証しながら、ネットワークへのアクセスを認められた特定のユーザーに、より柔軟なサービスを企業内のネットワークから提供することができる。

【０００６】しかし、企業内のネットワークとインターネットを接続して利用する場合に、上述の技術を利用しても依然として企業内ネットワークとインターネットで安全にデータを共有をすることは難しい。

【０００７】なお、インターネットを安価な通信媒体として利用する場合には、通信経路からのデータ漏洩から守るために、送信データを暗号化して送信することが行なわれているが、このようなデータの暗号／復号化は、システムのいろいろなレベルで行なわれている。例えば、通信ソケットレベルで行なわれる暗号化サービスとしてＳＳＬ（ｓｅｃｕｒｅ　ｓｏｃｋｅｔｓ　ｌａｙｅｒ）が知られており、また、特開平９－２５１４２６のようにファイルシステムというアプリケーションレベルでデータの暗号／復号化する技術が知られている。

【０００８】

【発明が解決しようとする課題】本発明は、上記した従来技術の欠点を除くためになされたものであって、その目的とするところは、安全に企業内ネットワークとインターネットでデータ共有を実現するデータ共有機構と、共有データを利用するアプリケーションの管理方法及び装置を提供することである。つまり、本発明は、企業内ネットワークあるいはインターネットのいずれからも、共有データにアクセス可能な構成と、企業内ネットワーク内のアプリケーションとインターネット上のアプリケーションが、アプリケーションの管理方法によって共有データを参照／更新して、等価なサービスを各々のネットワークに対して与える構成とを提供することを課題とする。

【０００９】

【課題を解決するための手段】この発明に係るデータ共有コンピュータシステムは、第一のコンピュータシステムと、第二のコンピュータシステムと、共有データ記憶部と、アクセス可否情報記憶部とを備えるデータ共有コンピュータシステムであって、（Ａ）共有データ記憶部は、複数のデータ記憶領域を有し、第一のコンピュータシステム及び第二のコンピュータシステムからアクセスされる共有データを、複数のデータ記憶領域に分割して記憶し、（Ｂ）アクセス可否情報記憶部は、共有データ記憶部の各データ記憶領域に対応して、そのデータ記憶領域に対してアクセス可能あるいはアクセス不可であることを意味するアクセス可否情報を記憶し、（Ｃ）第一のコンピュータシステムは、第一のサービス部と、共有データ記憶部に接続する第一のデータアクセス部と、アクセス可否情報記憶部に接続する第一の排他制御部とを備え、（１）第一のサービス部は、第一のデータアクセス部と第一の排他制御部に対して、任意のデータ記憶領域に対するアクセスを指示し、（２）第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更し、（３）第一のデータアクセス部は、第一の排他制御部により、アクセス可能と判定され、アクセス可否情報をアクセス不可に変更された後に、指示されたデータ記憶領域にアクセスし、（４）第一の排他制御部は、第一のデータアクセス部により、指示されたデータ記憶領域に対してアクセスされた後に、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更し、（Ｄ）第二のコンピュータシステムは、第二のサービス部と、共有データ記憶部に接続する第二のデータアクセス部と、アクセス可否情報記憶部に接続する第二の排他制御部とを備え、（１）第二のサービス部は、第二のデータアクセス部と第二の排他制御部に対して、任意のデータ記憶領域に対するアクセスを指示し、（２）第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更し、（３）第二のデータアクセス部は、第二の排他制御部により、アクセス可能と判定され、アクセス可否情報をアクセス不可に変更された後に、指示されたデータ記憶領域にアクセスし、（４）第二の排他制御部は、第二のデータアクセス部により、指示されたデータ記憶領域に対してアクセスされた後に、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更することを特徴とする。

【００１０】また、第一のコンピュータシステムは、第

三のコンピュータシステムを有する第一のネットワークシステムに接続し、第一のサービス部は、第一のネットワークシステムを介して第三のコンピュータシステムに対してサービスを提供し、第二のコンピュータシステムは、第四のコンピュータシステムを有する第二のネットワークシステムに接続し、第二のサービス部は、第二のネットワークシステムを介して第四のコンピュータシステムに対してサービスを提供することを特徴とする。

【００１１】また、第二のサービス部は、第一のサービス部が第一のネットワークシステムを介して第三のコンピュータシステムに対して提供するサービスと等価のサービスを、第二のネットワークシステムを介して第四のコンピュータシステムに対して提供することを特徴とする。

【００１２】また、第一の排他制御部は、バスロック機能付きバスによって、アクセス可否情報記憶部に接続し、第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する間、バスをロックし、第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更する間、バスをロックし、第二の排他制御部は、上記バスロック機能付きバスによって、アクセス可否情報記憶部に接続し、第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する間、バスをロックし、第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更する間、バスをロックすることを特徴とする。

【００１３】また、第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する一連の動作を、一の命令で実行し、第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する一連の動作を、一の命令で実行すること特徴とする。

【００１４】また、第一のコンピュータシステムは、以下の要素を備えることを特徴とする。

（１）データの暗号化及び復号化に用いる暗号鍵を記憶する暗号鍵記憶部、（２）暗号鍵を指定して暗号化を指示された場合には、指定された暗号鍵を用いてデータを暗号化し、暗号鍵を指定して復号化を指示された場合には、指定された暗号鍵を用いてデータを復号化するデータ暗号化／復号化実行部、（３）暗号鍵記憶部が記憶する暗号鍵を変更する暗号鍵再設定部、（４）第一のデータアクセス部に、データ記憶領域からの暗号データの読み出しを指示し、データ暗号化／復号化実行部に、変更前の暗号鍵を指定して、読み出した暗号データの復号化を指示し、データ暗号化／復号化実行部に、変更後の暗号鍵を指定して、復号化したデータの再暗号化を指示し、第一のデータアクセス部に、再暗号化したデータを、元のデータ記憶領域へ書き込むことを指示するデータ再暗号化部。

【００１５】この発明に係るクライアントは、ネットワークシステムに接続するクライアントであって、以下の要素を有することを特徴とする。

（１）上記ネットワークシステムに接続する第一のコンピュータシステムであって、第二のコンピュータシステムとデータを共有する第一のコンピュータシステムに対して、共有データを送信し、また、共有データを受信する共有データ送信／受信部、（２）データ送信／受信部が送信する共有データを暗号化するデータ暗号化部、（３）データ送信／受信部が受信した共有データを復号化するデータ復号化部。

【００１６】また、データ共有コンピュータシステムは、第三のコンピュータシステムを有し、第三のコンピュータシステムは、第一のコンピュータシステムが接続する第一のネットワークシステムに接続し、第一のサービス部は、第一のネットワークシステムを介して第三のコンピュータシステムに対してサービスを提供し、第三のコンピュータシステムは、第一のサービス部が提供するサービスによってアクセスした共有データをキャッシュする共有データキャッシュ部を有することを特徴とする。

【００１７】また、第一のサービス部は、第一の構成情報を用いて動作し、共有データ記憶部は、第一のサービス部が用いる第一の構成情報を記憶し、第二のコンピュータシステムは、他の記憶部を有し、第二のコンピュータシステムは、共有データ記憶部に記憶されている第一の構成情報を読み出し、読み込んだ第一の構成情報を他の記憶部に書き込む構成情報複製部を有し、第二のサービス部は、他の記憶部に書き込んだ第一の構成情報を更新し、更新した第二の構成情報を用いて動作することを特徴とする。

【００１８】また、第一のコンピュータシステムは、以下の要素を備えることを特徴とする。

（１）第一のコンピュータシステムによるユーザ認証の認証方式を記憶する認証方式管理部と、（２）認証に用いるデータを予め記憶する認証データベース管理部と、（３）認証要求と認証を受ける為のデータとを受付け、

認証を受ける為のデータと、認証データベース管理部に予め記憶された認証に用いるデータとを用いて、認証方式管理部に記憶された認証方式により、ユーザ認証を行なう認証機能部。

【００１９】また、データ共有コンピュータシステムは、バスを備え、第一のコンピュータシステムと、第二のコンピュータシステムと、共有データ記憶部と、アクセス可否情報記憶部とが上記バスに接続された共有メモリ型並列計算機であることを特徴とする。

【００２０】

【発明の実施の形態】以下本発明を図面に示す実施の形態に基づいて説明する。尚、図１から図１１に、主として各実施の形態におけるシステムの構成を示し、図１２から図４９に各実施の形態の動作に伴うデータフロー、処理フローやコマンドの構成等を示す。

実施の形態１．本発明によれば、クライアントサーバー型のサービスであって、アプリケーションプログラムとして実現されているものであれば、その既存のプログラムにほとんど変更を加えることなく、ネットワーク毎にそのサービスを複製して、それぞれネットワーク上で利用することが可能となる。例えば、ＩＭＡＰ４（ｉｎｔｅｒｎｅｔ ｍｅｓｓａｇｅ ａｃｃｅｓｓ ｐｒｏｔｏｃｏｌ ４）によるメールサービス、ＨＴＴＰ（ｈｙｐｅｒｔｅｘｔ ｔｒａｎｓｐｏｒｔ ｐｒｏｔｏｃｏｌ）サーバーサービスなどのサービスがこれに該当する。本実施の形態では、ファイルサーバーのサービスを複製し、利用する例を説明する。

【００２１】図１に、サービス複製システムのシステム構成図を示す。ここで、１０１は、構内ＬＡＮ（ｌｏｃａｌ ａｒｅａ ｎｅｔｗｏｒｋ）、１０２は、インターネット、１０３は、ＬＡＮ側サーバー、１０４は、共有ディスク、１０５は、インターネット側サーバー、１０６は、バスロック機能付きバス、１０７は、ＬＡＮ上のクライアントである。

【００２２】ＬＡＮ側サーバー１０３とインターネット側サーバー１０５とは、それぞれに独立したサーバー装置であるが、構内に隣接して設置され、各々ＳＣＳＩ（ｓｍａｌｌ ｃｏｍｐｕｔｅｒ ｓｙｓｔｅｍ ｉｎｔｅｒｆａｃｅ）にて共有ディスク１０４に接続し、共有するように構成されている。尚、ＳＣＳＩ以外に、ファイバチャネル等のより長い接続経路を許す技術を使用して共有ディスク１０４と接続する場合には、必ずしもサーバー装置同士を隣接する必要はない。

【００２３】バスロック機能付きバス１０６は、ＬＡＮ側サーバー１０３とインターネット側サーバー１０５とに接続し、サーバー装置間の共有メモリ機構に使用されるように構成されている。

【００２４】図２に、ＬＡＮ側サーバー１０３とインターネット側サーバー１０５の各サーバー装置上に配置されるソフトウェアの構成図を示す。２０１は、アプリケーションプログラム部、２０２は、ファイルシステム部、２０３は、ファイルサービス部、２０４は、ユーザー認証／認可管理部、２０５は、データ暗号／復号化実行部、２０６は、データ管理部である。

【００２５】アプリケーションプログラム部２０１は、ユーザー認証／認可管理部２０４とファイルサービス部２０３を呼び出して、アプリケーションを実行するように構成されている。ファイルサービス部２０３は、ファイルシステム部２０２を呼び出すように構成されている。ファイルシステム部２０２は、データ管理部２０６を呼び出すように構成され、データ管理部２０６は、データ暗号／復号化実行部２０５を呼び出すように構成されている。尚、ファイルサービス部２０３のサービスは、オペレーティングシステムのカーネルコードとして実行され、その処理コンテキストは１アプリケーションとして与えられるように構成されている。

【００２６】図３に、２０４ユーザー認証／認可管理部が、データ管理部２０６を用いて管理するユーザー認証／認可データベースのレコード例の図を示す。３０１は、ユーザーＩＤ、３０２は、そのユーザーのグループＩＤ、３０３は、そのユーザーのユーザーＩＤ、３０４は、そのユーザーの認証データ、３０５は、そのユーザーの共通秘密鍵である。ユーザーの共通秘密鍵は、データ管理部２０６がデータの暗号／復号化を行なう際に利用するものである。尚、ユーザー認証／認可管理部２０４は、ハッシュ関数によるパスワード参照の基本方式に加えて、チャレンジ方式と、ワンタイムパスワード方式を用意しており、ユーザー属性として認証方式の選択が可能なように構成されている。

【００２７】図４に、データ管理部２０６の構成図を示す。４０１は、排他制御部、４０２は、データ暗号／復号化指示部、４０３は、データアクセス部である。排他制御部４０１は、バスロック機能付きバス１０６を用いて共有メモリ機構にアクセスし、共有ディスク１０４のセクタ単位で、排他制御を行なうように構成されている。データ暗号／復号化指示部４０２は、共有ディスク１０４に書き込むデータの暗号化と、共有ディスク１０４から読み出したデータの復号化を、データ暗号／復号化実行部２０５に指示するように構成されている。データアクセス部４０３は、共有ディスク１０４のセクタ単位で、読み出しと、書き込みをするように構成されている。

【００２８】図５に、ロック中の共有ディスクセクタと共有メモリの状態の例の図を示す。５０１は、共有メモリ上のロックフィールド、５０２は、共有ディスク１０４上のセクタを示す。

【００２９】次に、この構成における基本的な動作について説明する。まず、図１２と図１３を用いて、システムログインの処理について説明する。図１２は、システムログインの処理フロー図である。図１３は、システム

ログイン処理のデータフロー図である。

【００３０】システムログインでは、ユーザー認証の処理を行ない（Ｓ１２０１）、ユーザー認証が成功した場合に、ログインセッションを生成する（Ｓ１２０２）。

【００３１】次に、図１４と図１５を用いて、ファイルオープンの処理について説明する。図１４は、ファイルサービス部２０３によるファイルオープンの処理フロー図である。図１５は、ファイルオープン処理のデータフロー図である。

【００３２】ファイルサービス部２０３は、クライアント１０７のクライアントプログラム部からファイルオープンの処理要求を受けると（Ｓ１４０１、１５０１）、ユーザー認証を行ない（Ｓ１４０２、１５０２、１５０３）、ユーザー認証が成功した場合に、ファイルシステム部２０２にオープン処理を依頼する（Ｓ１４０３、１５０４）。オープン処理の結果、ファイルシステム部２０２からファイル管理データ（通常、ｖｎｏｄｅと呼ばれる。）とクライアント認証キーを取得する（Ｓ１４０４、Ｓ１４０５、１５０５）。

【００３３】ファイルサービス部２０３は、取得したクライアント認証キーを記憶し（Ｓ１４０６）する。尚、これ以降にクライアント１０７からファイルサービス部２０３へデータアクセスの要求がされた場合には、ファイルサービス部２０３は、クライアントからの処理要求メッセージに含まれるクライアント認証キーと、記憶しているクライアント認証キーを比較することによって認証処理を行なう（Ｓ１６０３、Ｓ２３０３）。つまり、ユーザー認証／認可管理部２０４によらず、ファイルサービス部２０３自身が認証を行なう。

【００３４】ファイル管理データ（ｖｎｏｄｅ）は、ファイルシステム部２０２によってファイル毎に管理されるデータであって、ファイルのアクセス権、サイズ、オープンカウント、シークポインタ、ファイルデータの配置されるディスクブロックアドレスなどの情報の管理に用いられる。尚、このファイル管理データ（ｖｎｏｄｅ）は、ファイルサービス部２０３経由でアクセスする場合だけでなく、他のアプリケーションプログラムからファイルシステム部２０２に対してアクセスする場合にも用いられる。その場合、具体的にはファイルシステム部２０２に対して、ファイル管理データ（ｖｎｏｄｅ）に基づいたリード、ライト、シーク等のシステムコールを行なう。ファイルシステム部２０２は、そのシステムコールを解釈し、該当するディスク領域へアクセスする。

【００３５】ファイルサービス部２０３は、インデクスとクライアント認証キーとファイルオープン終了結果をクライアントプログラム部へ送信して（Ｓ１４０６、Ｓ１４０７、Ｓ１４０８、１５０６）、ファイルオープンの処理を終了する。

【００３６】次に、図１６から図２１を用いて、リードの処理について説明する。図１６は、ファイルサービス部２０３によるリードの処理フロー図である。図１７は、リード要求メッセージの例を示す図である。図１８は、ファイルシステム部２０２によるリードの処理フロー図である。図１９は、データ管理部２０６によるリードの処理フロー図である。図２０は、共有ディスク領域のリードセクタに対するロック取得の処理フロー図である。図２１は、共有ディスク領域のリードセクタに対するロック開放の処理フロー図である。図２２は、リード処理のデータフロー図である。

【００３７】ファイルサービス部２０３は、ＵＤＰ（ｕｓｅｒ ｄａｔａｇｒａｍ ｐｒｏｔｏｃｏｌ）の既知ポートをクライアントプログラム部に提供し、同ポートに対してクライアント１０３からの処理要求を受け付けることにより、ファイルサービスを行なう。クライアントプログラム部は、リードに相当する要求メッセージをファイルサービス部２０３に送信し、ファイルサービス部２０３は、メッセージを解釈してサービスを提供する（Ｓ１６０１、２２０１）。

【００３８】リード要求メッセージは、図１７のようなフォーマットで構成される。１７０１は、ファイル管理データ（ｖｎｏｄｅ）へのポインタの配列へのインデクス、１７０２は、ユーザーＩＤ、１７０３は、クライアント認証キー、１７０４は、サービス内容（ここで、１はリードを意味する。）、１７０５は、リード開始セクタオフセット、１７０６は、リードセクタサイズである。

【００３９】図１６に示すように、ファイルサービス部２０３は、リード要求メッセージ中のクライアント認証キー１７０３を取得し（Ｓ１６０２）、ファイルオープン処理中に記憶した（Ｓ１４０６）クライアント認証キーと比較して、一致する場合には処理を続行する（Ｓ１６０３）。

【００４０】リードするデータ領域が、共有ディスク１０４上の共有ディスクデータ領域の場合には、サーバー装置内の他のファイルシステムではなく、その共有データ領域を管理するデータ管理部２０６を用いるファイルシステム部２０２を選択する（Ｓ１６０５、Ｓ１６０７）。

【００４１】ファイルサービス部２０３は、メモリ領域を確保し（Ｓ１６０８）、ファイルシステム部２０２にリード要求を出す（Ｓ１６０９、２２０２）。このとき、同時にファイル管理データ（ｖｎｏｄｅ）へのポインタ、リード開始セクタオフセット、リードセクタサイズ、確保したメモリ領域の先頭アドレスを渡す。通常、ユーザーからのファイルシステム部２０２へのアクセスは、システムコール経由で行なわれるが、この場合のリード要求では、ファイルシステム部２０２の内部関数を利用して行われる。

【００４２】図１８に示すように、ファイルシステム部

２０２は、リード要求を受けとると（Ｓ１８０１、２２０２）、ファイル管理データ（ｖｎｏｄｅ）中のリード開始セクタオフセットを、データ管理部２０６で管理するリードセクタアドレスに変換し（Ｓ１８０２）、データ管理部２０６に対してリード要求を出す（Ｓ１８０３、２２０３）。このとき同時に、ユーザーＩＤ、リードセクタアドレス、リードセクタサイズ、メモリ領域の先頭アドレスを渡す。

【００４３】図１９に示すように、データ管理部２０６は、リード要求を受付け（Ｓ１９０１、２２０３）、排他制御部４０１により、共有ディスク領域のリードセクタのロック取得を行なう（Ｓ１９０２）。

【００４４】排他制御部４０１がアクセスする共有メモリ機構は、バスロック機能付きバス１０６を用いて、バスロックと１ビット毎のデータ参照更新とをできるだけのハードウェア構成で実現されている。排他制御部４０１は、このハードウェア構成を利用し、共有メモリ機構上のバイトアドレスを共有ディスク上のセクタアドレスにマッピングしている。

25

【００４５】図２０の示すように、排他制御部４０１は、リードセクタアドレスとリードセクタサイズを受けとると（２２０４）、バスロックを施して（Ｓ２００１、２２０５）、連続するリードセクタに対応するすべての共有メモリ機構上のバイトアドレス、つまりロックフィールドをチェックする（Ｓ２００２、２２０６）。リードセクタのうち一つでも使用中であることを示すロックフィールドがあれば、バスロックを解放して（Ｓ２００３、２２０５）、一定時間の休眠し（Ｓ２００４）、その後リトライを繰り返す。総てのロックフィールドがリードセクタの未使用を示している場合には、排他制御部４０１は、バスロック状態のまま、それらのロックフィールドに１（１は、ロックフィールドに対応するセクタが使用中であること示す。）を書き込む（Ｓ２００５、２２０６）。その後、バスロックを解放する（Ｓ２００６、２２０５）。

【００４６】図５に、ロック中の共有ディスクセクタと共有メモリの状態の例を示する。共有メモリのロックフィールド５０１の先頭は、共有ディスク上の１番目のセクタと対応していることを意味する。この例では、７番目から１１番目のロックフィールドが使用中となっている。そのため、７番目から１１番目のロックフィールドに対応する共有ディスク上の７セクタから１１セクタまでは、ロック状態にあり、ロック取得したユーザー以外は、これらのセクタに対してアクセスすることができないことを意味している。

【００４７】データ管理部２０６は、データアクセス部４０３により、リードセクタからディスクデータの読み出し（Ｓ１９０３、２２０８、２２０９）、アドレスを指定されたメモリ領域に格納する（２２１０）。

【００４８】データ管理部２０６は、読みだしが終了すると、排他制御部４０１により、ロックの解放を行なう（Ｓ１９０４）。ロックの解放は、図２１に示すように、バスロックを取得した上で（Ｓ２１０１、２２０５）、ロックフィールドに０を書き込むことにより行なわれる（Ｓ２１０２、２２０６）。その後、バスロックは解放される（Ｓ２１０３、２２０５）。

【００４９】データ管理部２０６は、データ暗号／復号化指示部４０２により、メモリ領域に読み込んだデータを復号化する（Ｓ１９０５）。データ暗号／復号化指示部４０２は、ファイルシステム部２０２から与えられたユーザーＩＤを指定して、ユーザー認証／認可管理部２０４からそのユーザーの共通秘密鍵３０５を得る。データ暗号／復号化指示部４０２は、この共通秘密鍵３０５を用いて、データ暗号／復号化実行部に復号化を実行させる（２２１２、２２１３、２２１４）。復号化したデータをメモリ領域に書き込み（Ｓ１９０６、２２１５）、ファイルシステム部２０２へリターンする（Ｓ１９０７、２２１６）。

【００５０】ファイルシステム部２０２は、ファイルサービス部２０３へリターンする（Ｓ１８０５、２２１８）。

【００５１】ファイルサービス部２０２は、リード要求を受けたクライアントプログラムのポートに読み出したデータを返送して、リード処理を終了する（Ｓ１６１１、２２１９）。

【００５２】次に、図２３から図２９を用いて、ライトの処理について説明する。図２３は、ファイルサービス部２０３によるライトの処理フロー図である。図２４は、ライト要求メッセージの例を示す図である。図２５は、ファイルシステム部２０２によるライトの処理フロー図である。図２６は、データ管理部２０６によるライトの処理フロー図である。図２７は、共有ディスク領域のライトセクタに対するロック取得の処理フロー図である。図２８は、共有ディスク領域のライトセクタに対するロック開放の処理フロー図である。図２９は、リード処理のデータフロー図である。

【００５３】ファイルサービス部２０３は、リードの処理と同様に、ライト要求メッセージを受け付ける（Ｓ２３０１、２９０１）。ライト要求メッセージは、図２４のようなフォーマットで構成される。２４０１は、ファイル管理データ（ｖｎｏｄｅ）へのポインタの配列へのインデクス、２４０２は、ユーザーＩＤ、２４０３は、クライアント認証キー、２４０４は、サービス内容（ここで、０はライトを意味する。）、２４０５は、ライト開始セクタオフセット、２４０６は、ライトセクタサイズ、２４０７は、ライトデータ列である。

【００５４】ライト要求は、リードの処理と同様に、ファイルシステム部２０２に渡され（Ｓ２３０９、２９０２）、ファイルシステム部２０２は、データ管理部２０６に、ユーザーＩＤ、ライトセクタアドレス、ライトセ

クタサイズ、ライトデータを格納したメモリ領域の先頭アドレスを渡す（Ｓ２５０３、２９０４）。リードの処理と同様に、データ暗号／復号化指示部２０５は、ユーザーＩＤに基づいてユーザーの共通暗号鍵３０５を得て、データ暗号／復号化実行部２０５に、データの暗号化を実行させる（Ｓ２６０３、２９０９～２９１２）。また、リードの処理と同様に、排他制御部４０１は、共有ディスク領域のライドセクタのロック取得を行ない（Ｓ２６０４、２９０６、２９０７）、データアクセス部４０３は、暗号データを書き込み（Ｓ２６０５、２９１５、２９１６）、その後排他制御部４０１は、ロックを解放する（Ｓ２６０６、２９０６、２９０７）。

【００５５】本実施の形態によれば、例えば企業内ネットワークとインターネットで安全にデータを共有でき、ネットワーク毎にサービスを複製して利用することができる。

【００５６】実施の形態２．次に、共有メモリ型並列計算機上でネットワーク毎にパーティショニングされたシステムについて説明する。図６は、並列計算機のシステム構成例である。ここで、６０１、６０２は、ＣＰＵ、６０３、６０４は、イーサネットコントローラ、６０５は、メモリ、６０６は、ディスクコントローラ、６０７は、ディスクであり、６０８は、メモリバスである。

【００５７】メモリバス６０８には、ＣＰＵ６０１、６０２、イーサネットコントローラ６０３、６０４、メモリ６０５、ディスク６０７が接続されている。ＣＰＵはテストアンドセット命令を備え、ＣＰＵから各デバイスへのアクセス、デバイスからＣＰＵへの割り込みは、メモリバス上の特定のアドレスにマッピングされたレジスタ経由で行なわれる様に構成されている。テストアンドセット命令については、後述する。

【００５８】メモリ６０５とディスク６０７の一部には、共有メモリ領域と共有ディスク領域が設けられている。ＬＡＮに接続されるイーサネットコントローラ６０３に接続され、ＬＡＮに所属するＣＰＵ６０１と、インターネットに接続されるイーサネットコントローラ６０４に接続され、インターネットに所属するＣＰＵ６０２とは、仮想空間で隔離され、各ネットワークに固有のメモリ領域、および、お互いのイーサネットコントローラにアクセスすることはできないように構成されている。

【００５９】次に、図３０を用いて、この構成における基本的な動作について説明する。このシステムは、リセットされると、ＣＰＵ６０１のみが、仮想記憶をディスエーブルした状態でＲＯＭコードの実行を始める。この時、ＣＰＵ６０２はディスエーブル状態となっている。

【００６０】ＣＰＵ６０１は、メモリプローブチェックを実行して使用可能なメモリ量を得て（Ｓ３００１）、ブートコードをロードし、実行する（Ｓ３００２）。ブートコードの実行により、メモリ量をチェックして、図７に示すようにメモリ領域を分割する（Ｓ３００３）。図７は、メモリ区分の例である。７０７は、ＬＡＮに所属するＣＰＵ６０１の使用するメモリ領域、７０８は、インターネットに所属するＣＰＵ６０２の使用するメモリ領域、７０９は、排他制御のために使用する共有メモリ領域である。

【００６１】メモリ領域の分割を決定すると、次に各々のＣＰＵの仮想空間を形成するページテーブルのセットアップを行なう（Ｓ３００４）。ＣＰＵ６０１のメモリ領域７０７では、イーサネットコントローラ６０３のレジスタ領域へのページテーブルエントリ７０１、共有ディスクのコントローラレジスタ領域へのページテーブルエントリ７０２、共有メモリ領域へのページテーブルエントリ７０３、および、ＣＰＵ６０１のカーネルコード使用領域のページテーブルエントリをセットアップする。同様に、ＣＰＵ６０２のメモリ領域７０８では、イーサーネットコントローラ６０４のレジスタ領域へのページテーブルエントリ７０４、共有ディスクのコントローラレジスタ領域へのページテーブルエントリ７０５、共有メモリ領域へのページテーブルエントリ７０６、および、ＣＰＵ６０２のカーネルコード使用領域のページテーブルエントリをセットアップする。

【００６２】カーネルの仮想空間は、図７に示したページテーブルエントリを除き、２つの領域で同等にセットアップされ、同一のカーネルコードが同一のカーネル仮想アドレスにロードされる。ＣＰＵ６０２は、仮想記憶をイネーブルし、カーネルコードのスタートアドレスから実行を開始する。また、ＣＰＵ６０１も、仮想記憶をイネーブルし、自身のスタートアドレスにジャンプして、カーネルコードの実行を開始する（Ｓ３００６、Ｓ３００７）。

【００６３】実施の形態１で示したソフトウエアと同一のソフトウェアが、各々のＣＰＵで実行されるが、排他制御部４０１の処理方式については、実施の形態１と異なり、本実施の形態の特徴を有する。実施の形態１では、共有メモリバスのバスロック機構を用いて、共有ディスク領域のリードセクタのロック取得とロック解放の処理を行なったが、本実施の形態では、図３１に示すように、共有メモリ６０５上のロックフィールドに対してのロック取得とロック解放の処理をテストアンドセット命令によるロック機構を用いて行なう。テストアンドセット命令とは、メモリ上のデータに対してアトミックに参照更新を行なえる命令である。図３２に示すように、ロック取得の処理の場合は、当該ロックフィールドに対して１をセットすることにより行なう（Ｓ３２０１）。そして、同命令で得られた値が０である場合には、ロック取得処理の成功を意味し（Ｓ３２０３）、１の場合には、すでに他者がロック取得済みであったため、ロック取得処理が失敗したことを意味する（Ｓ３２０４）。また、ロック解放の処理は、テストアンドセット命令でロックフィールドを０に書き戻すことで行なわれる。

【００６４】このように本実施の形態によれば、共有メモリ型並列計算機上でネットワーク毎にパーティショニングされたシステムを実現し、各々のネットワークから他者ネットワークへの侵害を排除することによって、システムの安全性を向上させることができる。

【００６５】実施の形態３．本実施の形態では、複数のネットワークから参照できる共有ディスク上の暗号化データを、定期的に異なるキーを用いて再暗号化する機構について説明する。

【００６６】実施の形態１で説明したように、ユーザー認証／認可管理部２０３は、図３に示すような共通秘密暗号鍵３０５を含むレコードからなるユーザー認証／認可データベースを管理し、ユーザーが登録時に暗号鍵を設定することにより、データを暗号化して保存することを可能にしている。本実施の形態では、それに加えてユーザーがシステムの提供する暗号鍵再設定／再暗号化コマンド（ｓｅｔｅｎｃｋｅｙコマンドという。）を利用することにより、暗号鍵の変更、およびその暗号鍵によるデータの再暗号化を行なうことを可能にする。

【００６７】ｓｅｔｅｎｃｋｅｙコマンドは、安全性を高めるために、イントラネット側のサーバー１０５、あるいはオペレーティングシステムにのみ用意される。また、さらに安全性を高めるためは、後述する再暗号化ＡＰＩ（ａｐｐｌｉｃａｔｉｏｎ ｐｒｏｇｒａｍｍｉｎｇ ｉｎｔｅｒｆａｃｅ）をイントラネット側サーバー１０５にのみ備える構成とすることも有効である。

【００６８】次に、図３３から図３８を用いて、暗号鍵再設定及びデータの再暗号化を実行する基本的な動作について説明する。ユーザーは、ユーザー認証を経て、イントラネット側サーバー１０５にログインを実行し（Ｓ３３０１）、図３４のようなｓｅｔｅｎｃｋｅｙコマンドを実行させる（Ｓ３３０２）。ここで、３４０１は、新暗号鍵を意味する。

【００６９】図３５を用いてｓｅｔｅｎｃｋｅｙの処理を説明する。ｓｅｔｅｎｃｋｅｙコマンドの実行により、ユーザー認証／認可管理部２０４は、ユーザー認証／認可データベース中のレコードの暗号鍵を指定された新暗合鍵に変更する（Ｓ３５０１、Ｓ３５０２）。

【００７０】その後、ファイルシステムに対して、図３６に示すような特殊ＡＰＩシステムコールｓｅｔｕｓｅｒａｔｒを発行する（Ｓ３５０３）。３６０１は、ユーザーＩＤ、３６０２は、旧暗号鍵、３６０３は、新暗号鍵であり、図３に示すレコードを例とすると、ユーザーｓａｋａｋｕｒａの旧暗号鍵０１２８０９０９を新暗号鍵０１０１０１０１に変更せよという意味である。

【００７１】図３７を用いて、ｓｅｔｕｓｅｒａｔｒの処理を説明する。システムコールｓｅｔｕｓｅｒａｔｒの実行により、ファイルシステム部２０２は自らが管理するファイルのうちそのユーザーがオーナーであるファイルを全検索する（Ｓ３７０１）。データ管理部２０６に対して、発見したそのユーザーのファイルが使用するセクタを対象に、再暗号化コマンドｒｅｅｎｃを発行する（Ｓ３７０２）。具体的には、再暗号化コマンドｒｅｅｎｃに、旧暗号鍵、新暗号鍵、更新セクタチャンク数、セクタアドレス、とセクタサイズのセクタチャンク数分のエントリを有する配列を引数として渡してコールする。

【００７２】図３８を用いて、ｒｅｅｎｃの処理について説明する。ｒｅｅｎｃの処理では、実施の形態１で述べたデータ管理部２０６によるリードやライトのオペレーションと同様に、配列で示された当該セクタすべてのロックを取得する（Ｓ３８０１）。その後すべてのセクタデータに対し読み出しを行ない（Ｓ３８０２）、データ暗号／復号化機能を使用して旧暗号鍵で復号した後（Ｓ３８０３）、新暗号鍵で再暗号化して（Ｓ３８０４）、当該ディスクへの書き戻しを行なう（Ｓ３８０５）。すべての当該セクタにつき書換えが終了すると、取得したすべてのロックを解放し（Ｓ３８０６）、ファイルシステム部２０２にリターンする。

【００７３】システムコールを終了し、ユーザー認証／認可管理部２０４にリターンし、ｓｅｔｅｎｃｋｅｙコマンドの実行を終了する。

【００７４】前述の実施の形態におけるサーバー装置は、ユーザー認証により第三者からの不法なアクセスからシステムを保護するように構成されているが、本実施の形態にかかる再暗号化機構は、万が一第三者に不法なログインを許してしまった場合に備え、データ秘匿性を高めることができる点で有効である。

【００７５】実施の形態４．本実施の形態では、サーバー上に保管されている暗号化データをクライアント上で復号化し、データの秘匿安全性を向上させる形態について説明する。

【００７６】図８に、サーバー装置を利用するクライアントのソフトウェア構成図を示す。８０１は、クライアントプログラム上で動作するクライアント側アプリケーションプログラム部、８０２は、実施の形態１、２のファイルサービス部２０３に対するクライアントとしての機能を含むクライアント側ファイルシステム部、８０３は、データ暗号／復号化実行部２０５と同等の機能を有するクライアント側データ暗号／復号化実行部である。例えば、クライアントに携帯端末を用いる場合には、一つのクライアントに対してユーザーは一人しかいないことになる。

【００７７】クライアント側アプリケーションプログラム部８０１は、実施の形態１のサーバー上のアプリケーションプログラム部と同様にクライアント側ファイルシステム部８０２に対してファイルの読み書き操作を行なうように構成されている。

【００７８】次に、図３９から図４１を用いて本実施の形態における基本的な動作について説明する。図３９

は、オープン処理のデータフロー図である。クライアント側ファイルシステム部８０２は、ｏｐｅｎシステムコール３９０１を解釈し、サーバー装置上のファイルサービス部２０３のＵＤＰ（ｕｓｅｒ　ｄａｔａｇｒａｍ　ｐｒｏｔｏｃｏｌ）の既知ポートに対して、「暗号／復号化なし」の属性でオープンメッセージを送信する（３９０２）。ｖｎｏｄｅ中に「暗号／復号化不要」のデータが含まれる以外は、実施の形態１と同様に処理される。「暗号／復号化不要」の属性でオープンしている間には、「暗号／復号化必要」な処理は許されず、逆に「暗号／復号化必要」の属性でオープンしている間には、「暗号／復号化不要」な処理は許さない。

【００７９】図４０は、リード処理のデータフロー図である。クライアント側ファイルシステム部８０２は、ファイルオープンに引続きリードシステムコールを受けとると（４００１）、ファイルサービス部２０３にリード要求メッセージを送信する（４００２）。ファイルサービス部２０３は、ファイルシステム部２０２にリード要求を出す（４００３）。ファイルシステム部２０２は、ｖｎｏｄｅが「暗号／復号化不要」となっているので、データ管理部２０６に対して、復号化無リード要求を発行する（４００４）。データ管理部２０６からの復号化無リード要求に対する処理は、復号化処理を行なわない点を除き実施の形態１で説明したリード処理と全く同じに動作する。このようにして、暗号化されたままのデータが、クライアント１０７に、実施の形態１での返送メッセージと同じ態様で返送される（４０１６）。

【００８０】クライアント側では返送された暗号化データを受けとると、クライアント側ファイルシステム部８０２が、コンフィグレートされた暗号鍵を用いてデータ暗号／復号化実行部８０３に復号化を実行させる（４０１６）。クライアント側ファイルシステム部８０２は、復号化されたデータをクライアント側アプリケーションプログラム部８０１に返してリード処理を終了する（４０１８）。

【００８１】図４１は、ライト処理のデータフロー図である。クライアント側ファイルシステム部８０２は、ライトシステムコールを受けとると（４１０１）、暗号鍵を用いて受けとったデータをデータ暗号／復号化実行部８０３に暗号化させる（４１０２、４１０３）。クライアント側ファイルシステム部８０２は、暗号化されたデータとライト要求メッセージをファイルサービス部２０３に送信する（４１０４）。ファイルサービス部２０３は、ファイルシステム部２０２へライト要求を発行する（４１０６）。ファイルシステム部２０２は、データ管理部２０６に対して暗号化無ライト要求をコールする（４１０７）。実施の形態１で説明したデータ管理部２０６は、暗号化せず、そのままデータを書き込む（４１１３、４１１４）。ファイルサービス部２０３は、処理の完了をクライアント１０７に報告する（４１１７）。

【００８２】このようにクライアント上にデータの暗号／復号化機能を置くことにより、データの秘匿安全性を向上することができる。特に、携帯クライアント端末から無線通信にてサーバと通信する場合に、データの秘匿安全性を確保することができる点で有効である。

【００８３】実施の形態５．本実施の形態では、遠隔地からインターネットを介して、本発明に係る複製サービスを利用する場合に、データ転送遅延を小さくするシステムについて説明する。具体的には、代理サーバーを設け、実施の形態１で説明したファイルサービスのデータキャッシュ機能を実現する例を説明する。

【００８４】図９は、実施の形態５に係るシステム構成を示す図である。１０５は、実施の形態１で説明したインターネット側サーバー（複製サーバー）１０５、９０１は、代理サーバー、９０２は、ＬＡＮ、９０３と９０４は、クライアントである。クライアント９０３、９０４は、インターネット１０２を介してインターネット側サーバー１０５からサービスの提供を受ける。

【００８５】代理サーバー９０１が提供するファイルサービスは、クライアント９０３、９０４からみて、インターネット側サーバー１０５のファイルサービス部２０３に直接接続した場合のファイルサービスと全く同等になるように構成される。そのため代理サーバー９０１は、インターネット側サーバー１０５のファイルサービス部２０３が提供しているＵＤＰの既知ポートと同一番号のポートをクライアント９０３、９０４に対して提供している。

【００８６】次に、この構成における基本的な動作について説明する。まず、オープン処理について説明する。図４２は、オープン処理のデータフロー図である。４２５１は、クライアントプログラム部、４２５２は、代理サーバー側ファイルサービス部である。

【００８７】クライアントプログラム部４２５１は、代理サーバー９０１の前記既知ポートにファイルオープンメッセージを送信する（４２０１）。代理サーバー側ファイルサービス部４２５２は、ファイルオープンメッセージを受けとると、内部データ（ファイルエントリ、セクタ管理テーブル及びセクタデータ領域）を用意する。

【００８８】図１０は、内部データ（ファイルエントリ、セクタ管理テーブル及びセクタデータ領域）の構成を示す図である。１００１は、ファイルエントリである。そのうち、１００２は、ユーザーＩＤフィールド、１００３は、ファイル名フィールド、１００４は、クライアント認証キーフィールド、１００５は、ファイルオープン属性フィールド、１００６は、ファイルのオープンアカウントフィールド、１００７は、先頭セクタの管理テーブルへのポインタフィールドである。また、セクタ管理テーブルは、１００８のファイルのセクタ番号、１００９の次管理テーブルへのポインタ、１０１０のセクタデータ領域へのポインタから構成される。１０１１

は、セクタデータ領域である。

【００８９】代理サーバー側ファイルサービス部４２５２は、ファイルオープンメッセージ中のユーザーのＩＤとオープンするファイル名を、それぞれユーザーＩＤフィールド１００２とファイル名フィールド１００３に格納する（４２０２）。また、ファイルオープン属性をファイルオープン属性フィールド１００５に格納する（４２０２）。このファイルオープン属性には、実施の形態４で説明した「暗号／復号化必要」あるいは「暗号／復号化不要」の属性が含まれる。

【００９０】ファイルオープンメッセージは、そのままインターネット側サーバー１０５のファイルサービス部２０３に転送され（４２０３）、代理サーバー側ファイルサービス部４２５２は、ファイルサービス部２０３からの返送メッセージ中にあるクライアント認証キーをクライアント認証キーフィールド１００４に格納する（４２０２）。また、本ファイルのオープンカウントは、ファイルのオープンアカウントフィールド１００６に格納される（４２０２）。

【００９１】次に、リード処理について説明する。図４３は、リード処理の処理フロー図である。図４４は、リード処理のデータフロー図である。代理サーバー側サービス部４２５２は、クライアントプログラム部４２５１からのリード要求メッセージを受けとると（Ｓ４３０１、４４０１）、先頭セクタの管理テーブルへのポインタフィールド１００７をチェックする（Ｓ４３０２、４４０２）。このフィールドに０ｘｆｆｆｆｆｆｆｆが格納されている場合（先頭セクタの管理テーブルへのポインタがセットされていないことを意味する。）には、このファイルは、リード処理が実行されていないと判断し、クライアントプログラム部４２５１からのメッセージをインターネット側サーバー１０５のファイルサービス部２０３に転送する（Ｓ４３０３、４４０３）。

【００９２】代理サーバー側サービス部４２５２は、リードデータを取得し（Ｓ４３０４、４４０４）、返送メッセージをクライアントプログラム部４２５１に転送する（Ｓ４３０５、４４０５）。

【００９３】代理サーバー側サービス部４２５２は、図１０に示すように必要なセクタデータ領域１０１１とそれに対応するセクタ管理テーブル１００８、１００９、１０１０を確保する（Ｓ４３０６、Ｓ４３０７、４４０６、４４０７）。先頭セクタの管理テーブルへのポインタフィールド１００７に、先頭セクタの管理テーブルへのポインタを格納し、（Ｓ４３０８、４４０８）。ファイルのセクタ番号フィールド１００８に、対応するファイルのセクタ番号を格納し（Ｓ４３０９、４４０７）、セクタデータ領域へのポインタフィールド１０１０に、セクタデータ領域へのポインタを格納し（Ｓ４３１０、４４０７）、セクタデータ領域１０１１に返送メッセージから得たリードデータを格納する（Ｓ４３１１、４４０６）。

【００９４】２以上のセクタデータ領域を必要とする場合には（Ｓ４３１２）、次管理テーブルへのポインタフィールド１００９に、次管理テーブルへのポインタを格納し（Ｓ４３１３、４４０７）、これによって管理テーブルをリンクし、管理テーブルが最終の場合には（Ｓ４３１２）、次管理テーブルへのポインタフィールド１００９に、０ｘｆｆｆｆｆｆｆｆを格納する（Ｓ４３１４、４４０７）。

【００９５】これ以降代理サーバーへのこのファイルに対するリード要求が発生した場合に、図１０に示すキャッシュ上に既に該当するセクタが存在すれば（Ｓ４３０２）、そのデータをそのまま利用する（Ｓ４３１５～Ｓ４３１９）。セクタが存在しないければ（Ｓ４３２０）、不足分のセクタデータをインターネット側サーバ１０５のファイルサービス部２０３に要求して（Ｓ４３０３）、既存セクタデータのリンクに挿入する（Ｓ４３１３、Ｓ４３０９～Ｓ４３１２）。リード要求にあるセクタがすべて揃った時点で、ファイルサービス部２０３が生成するのと同じ形態のリード要求返送メッセージを作成し、クライアントプログラム部に返す（４２０５、４４０５）。

【００９６】次にライト処理について説明する。図４５は、ライト処理の処理フロー図である。図４６は、ライト処理のデータフロー図である。クライアントプログラム部４２５１からのライト要求メッセージを代理サーバー側ファイルサービス部４２５２が受けとると（Ｓ４５０１、４６０１）、代理サーバー側ファイルサービス部４２５２は、このメッセージをインターネット側サーバー１０５のファイルサービス部２０３に転送する（Ｓ４５０２、４６０２）。すでにこのファイルのファイルエントリ１００１に、ライトするセクタのデータが保存されていれば（Ｓ４５０４、４６０４）、それらのセクタに対してクライアントプログラム部４２５１からのライト要求メッセージ中のセクタデータで上書きし（Ｓ４５０５、４６０５）、当該セクタのセクタデータ領域が確保されていなければ、新たなセクタデータ領域を確保して（Ｓ４５０７、４６０６、４６０７）、これらのリンクに挿入する（Ｓ４５０８、４６０７、４６０８）。

【００９７】次にファイルの無効化の処理について説明する。図４７は、ファイル無効化処理のデータフロー図である。あるファイルが代理サーバー９０１によってキャッシュされている場合に、ＬＡＮ側サーバー１０３から共有ディスク１０４上の対応するファイルの内容が更新されると、代理サーバー９０１上のファイルデータと共有ディスク１０４上の対応するファイルデータは、同一でなくなる。このような場合のファイルデータの一貫性維持のコントロールに関しては、クライアント９０３、９０４に任される。そのため、クライアント側アプリケーション部８０１は、代理サーバー９０１上のキャ

ッシュされたファイルデータを無効化したい場合に、クライアント側ファイルシステム部８０２に対して、無効化したいファイルを指定してｆｃｎｔｌシステムコールの無効化コマンドを発行する（４７０１）。

【００９８】クライアント側ファイルシステム部８０２は、無効化コマンドを解釈し、代理サーバー９０１に対し無効化要求を出す（４７０２）。図４８は、無効化要求メッセージの例を示す図である。

【００９９】代理サーバー側ファイルサービス部４２５２は、無効化要求メッセージを受けとると、自らが管理するファイルエントリを検索し（４７０３）、無効化するファイルのファイルエントリのファイルオープン属性１００５を０ｘｆｆｆｆｆｆｆｆにて初期化しキャッシュデータを無効化する（４７０４）。これにより、再びこのファイルに対するリード要求があった場合に、改めてインターネット側サーバー１０５のファイルサービス２０３からファイルデータを取得するようになる。

【０１００】ここで問題視するデータ転送遅延は、インターネット接続の距離が大きくなるにつれて増大する。例えば、日本とアメリカ西海岸では到達に０．２秒ほどかかる。この遅延時間を吸収するため、本発明は有効である。

【０１０１】実施の形態６．上述のように本発明を適用することにより、複数のネットワークに対して共通のファイルサービスが提供できる。このようなファイルサービスが提供するネットワーク間の共有ファイルを利用して、ファイル上のデータを基に動作するサーバーサービスを、従来のサーバープログラムを変更することなく提供することができる。例えば、ＩＭＡＰ４（ｉｎｔｅｒｎｅｔ　ｍｅｓｓａｇｅ　ａｃｃｅｓｓ　ｐｒｏｔｏｃｏｌ　４）メールサービスを複製すると、このサーバー機能がＳＭＴＰにてイントラネット内でメールデータを受けとり、共有ディスク上にサーバーの管理するデータとしてメールデータを保管する。このデータは共有ディスクに管理されるので、このメールデータを基にイントラネット、インターネット上でＩＭＡＰ４サービスを提供できる。これにより、ＩＭＡＰ４メールサービスのユーザーは、イントラネット（例えば、社内）からでも、インターネット（例えば、出先）からでもイントラネットのユーザーのメールアカウントに届いたメールを読んで処理することができるようになる。

【０１０２】ところが、同じサーバープログラムを使用するものの、ＩＭＡＰ４サーバーの設定に関して、イントラネット側ではメール取り込みが必要なのに対して、インターネット側ではメール取り込みが不要となる。つまり、設定ファイルの一部について、各ネットワーク毎に独自に設定する必要が生じ、別個に設定ファイルを設けなければならなくなる場合がある。

【０１０３】そのために本実施の形態では、そのような設定に必要なファイルローカライズ機構について説明する。サーバー装置の管理者は、ローカライズの必要なファイルに関して、以下のようなコマンドを出す。

Ｌｏｃａｌｉｚｅ　ａｆｉｌｅ

具体的には、設定ファイルをオープンした後、設定ファイルを指定してｆｃｎｔｌシステムコールにて上記コマンドを発行する。

【０１０４】図４９に、Ｌｏｃａｌｉｚｅコマンド処理のフロー図を示す。ファイルシステム部２０２は、ファイルシステム部２０２が管理している非共有ディスク領域に、新たなセクタ領域を確保し（Ｓ４９０１）、データ管理部２０６から設定ファイルのセクタデータを読み出して（Ｓ４９０２）、確保したセクタ領域に読み出したセクタデータを書き込む（Ｓ４９０３）。このようにして、ファイルデータを非共有領域にコピーする。新たに確保したセクタを管理するｉｎｏｄｅを参照するよう設定ファイルのｖｎｏｄｅを更新することにより（Ｓ４９０４）、ファイルシステム部は共有領域上のファイルのローカライズを行なう。

【０１０５】このようにして、ネットワーク毎にサービスの構成情報を独自に更新管理することが可能となる。

【０１０６】実施の形態７．本実施の形態では、本発明に係るサービス複製サーバー装置に関して、サーバー装置を構成するサブネットワーク毎にそのネットワークで必要とされる強度の認証機構を、必要に応じて構成することを可能とした認証機構について説明する。例えばイントラネットに関しては、一般に安全性確保のために外部のネットワークから厳重に保護されており、イントラネット内ではそれほど高い認証強度は要求されない。一方インターネットでは、常に外部の脅威に晒されており、高い認証強度が要求される。

【０１０７】図１１に本実施の形態に係るユーザー認証／認可管理部の構成図を示す。１１０１は、認証機能部、１１０２は、認可方式管理部、１１０３は、認証／認可データベース更新管理部、１１０４は、認証／認可データベース管理部である。これらの構成により、各々のサブネットワークが必要とする認証強度の認証機能をサブネットワーク毎に構成することができる。

【０１０８】認証機能部１１０１は、ユーザーからの認証要求を受けて認証を行なう。このとき、認証機能部１１０１は、認証方式管理部１１０３が管理する認証方式に従い、認証／認可データベース管理部１１０４から認証データを得て、照合することによって認証を行なう。

【０１０９】システム管理者は、認証方式管理部１１０２にサブネットワークが必要とする認証強度にふさわしい認証機能を導入設定しておくことができる。例えば、イントラネットに関しては、ＵＮＩＸ等で広く普及しているＭＤ５（ｍｅｓｓａｇｅｄｉｇｅｓｔ　ａｌｇｏｒｉｔｈｍ　５）のようにハッシュ関数認証を持った認証機能を導入設定し、一方インターネットに関しては、ワンタイムパスワードを用いた認証機能を導入設定するこ

とができる。

【０１１０】各認証機能は、認証機能部１１０１から認証検証すべきデータを得て、認証／認可データベース管理部１１０４から認証データを得て、認証するインターフェースを備えている。また、各認証機能は、共通の認証データを使用するよう構成されている。

【０１１１】認証／認可データベースは、各ネットワーク間で共有される。従って、システムのユーザー管理を行なうシステム管理者は、いずれかのサブネットワーク上の認証／認可データベース更新管理部１１０３に対して更新すれば足り、その更新内容は自動的にすべてのネットワークの認証機能に対して反映される。

【０１１２】

【発明の効果】本発明により、例えば企業内ネットワークとインターネットのように異なるネットワーク間で安全にデータを共有でき、ネットワーク毎にサービスを複製して利用することができる。

【０１１３】本発明では、共有メモリ型並列計算機上でネットワーク毎にパーティショニングされたシステムを実現しているので、各々のネットワークから他者ネットワークへの侵害を排除することによって、システムの安全性を向上させることができる。

【０１１４】本発明では、再暗号化機構により、万が一第三者に不法なログインを許してしまった場合に備え、データ秘匿性を高めることができる。

【０１１５】本発明では、クライアント上でデータを暗号／復号化することにより、データの秘匿安全性を向上することができる。特に、携帯クライアント端末から無線通信にてサーバと通信する場合に、データの秘匿安全性を確保することができる点で有効である。

【０１１６】本発明では、インターネット接続の距離が大きくなるにつれて増大するデータ転送遅延を吸収することができる。

【０１１７】本発明により、ネットワーク毎にサービスの構成情報を独自に更新管理することができる。

【０１１８】本発明により、サブネットワーク毎に必要とされる強度の認証機構を用いることができる。

【図面の簡単な説明】

【図１】　実施の形態１に係るサービス複製システムのシステム構成図である。

【図２】　実施の形態１に係る各サーバ装置上に配置されるソフトウェアの構成図である。

【図３】　実施の形態１に係るユーザ認証／認可データベースのレコード例の図である。

【図４】　実施の形態１に係るデータ管理部の構成図である。

【図５】　実施の形態１に係るロック中の共有ディスクセクタと共有メモリの状態の例の図である。

【図６】　実施の形態２に係る並列計算機のシステム構成例を示す図である。

【図７】　実施の形態２に係るメモリ区分の例の図である。

【図８】　実施の形態４に係るクライアントソフトウェア構成図である。

【図９】　実施の形態５に係るシステム構成を示す図である。

【図１０】　実施の形態５に係る内部データの構成を示す図である。

【図１１】　実施の形態７に係るユーザ認証／認可管理部の構成図である。

【図１２】　実施の形態１に係るシステムログインの処理フロー図である。

【図１３】　実施の形態１に係るシステムログイン処理のデータフロー図である。

【図１４】　実施の形態１に係るファイルオープンの処理フロー図である。

【図１５】　実施の形態１に係るファイルオープン処理のデータフロー図である。

【図１６】　実施の形態１に係るファイルサービス部によるリードの処理フロー図である。

【図１７】　実施の形態１に係るリード要求メッセージの例を示す図である。

【図１８】　実施の形態１に係るファイルシステム部によるリードの処理フロー図である。

【図１９】　実施の形態１に係るデータ管理部によるリードの処理フロー図である。

【図２０】　実施の形態１に係る共有ディスク領域のリードセクタに対するロック取得の処理フロー図である。

【図２１】　実施の形態１に係る共有ディスク領域のリードセクタに対するロック開放の処理フロー図である。

【図２２】　実施の形態１に係るリード処理のデータフロー図である。

【図２３】　実施の形態１に係るファイルサービス部によるライトの処理フロー図である。

【図２４】　実施の形態１に係るライト要求メッセージの例を示す図である。

【図２５】　実施の形態１に係るファイルシステム部によるライトの処理フロー図である。

【図２６】　実施の形態１に係るデータ管理部によるライトの処理フロー図である。

【図２７】　実施の形態１に係る共有ディスク領域のライトセクタに対するロック取得の処理フロー図である。

【図２８】　実施の形態１に係る共有ディスク領域のライトセクタに対するロック開放の処理フロー図である。

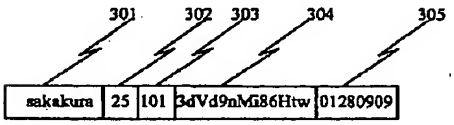
【図２９】　実施の形態１に係るリード処理のデータフロー図である。

【図３０】　実施の形態２に係る基本的な動作を示す図である。

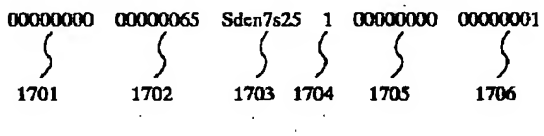
【図３１】　実施の形態２に係るテストアンドセット命令によるロック機構を示す図である。

【図３２】　実施の形態２に係るロック取得結果を判断するフロー図である。
【図３３】　実施の形態３に係るサーバ側の処理フロー図である。
【図３４】　実施の形態３に係るｓｅｔｅｎｃｋｅｙコマンドのフォーマット図である。
【図３５】　実施の形態３に係るｓｅｔｅｎｃｋｅｙの処理フロー図である。
【図３６】　実施の形態３に係るｓｅｔｕｓｅｒａｔｒのフォーマット図である。
【図３７】　実施の形態３に係るｓｅｔｕｓｅｒａｔｒの処理フロー図である。
【図３８】　実施の形態３に係るｒｅｅｎｃの処理フロー図である。
【図３９】　実施の形態４に係るオープン処理のデータフロー図である。
【図４０】　実施の形態４に係るリード処理のデータフロー図である。
【図４１】　実施の形態４に係るライト処理のデータフロー図である。
【図４２】　実施の形態５に係るオープン処理のデータフロー図である。
【図４３】　実施の形態５に係るリード処理の処理フロー図である。
【図４４】　実施の形態５に係るリード処理のデータフロー図である。
【図４５】　実施の形態５に係るライト処理の処理フロー図である。
【図４６】　実施の形態５に係るライト処理のデータフロー図である。
【図４７】　実施の形態５に係るファイル無効化処理のデータフロー図である。
【図４８】　実施の形態５に係る無効化要求メッセージの例を示す図である。
【図４９】　実施の形態６に係るＬｏｃａｌｉｚｅコマンド処理のフロー図である。
【符号の説明】
１０１　構内ＬＡＮ（ｌｏｃａｌ　ａｒｅａ　ｎｅｔｗｏｒｋ）、１０２　インターネット、１０３　ＬＡＮ側サーバー、１０４　共有ディスク、１０５　インターネット側サーバー、１０６　バスロック機能付きバス、１０７　クライアント、２０１　アプリケーションプログラム部、２０２　ファイルシステム部、２０３　ファイルサービス部、２０４　ユーザー認証／認可管理部、２０５　データ暗号／復号化実行部、２０６　データ管理部、３０１　ユーザーＩＤ、３０２　ユーザーのグループＩＤ、３０３　ユーザーＩＤ、３０４　ユーザーの認証データ、３０５　共通秘密鍵、４０１　排他制御部、４０２　データ暗号／復号化指示部、４０３　データアクセス部、５０１　共有メモリ上のロックフィールド、５０２　共有ディスク上のセクタ、６０１，６０２　ＣＰＵ、６０３，６０４　イーサネットコントローラ、６０５　メモリ、６０６　ディスクコントローラ、６０７　ディスク、６０８　メモリバス、７０１　イーサネットコントローラのレジスタ領域へのページテーブルエントリ、７０２　共有ディスクのコントローラレジスタ領域へのページテーブルエントリ、７０３　共有メモリ領域へのページテーブルエントリ、７０４　イーサーネットコントローラのレジスタ領域へのページテーブルエントリ、７０５　共有ディスクのコントローラレジスタ領域へのページテーブルエントリ、７０６　共有メモリ領域へのページテーブルエントリ、７０７　ＬＡＮに所属するＣＰＵの使用するメモリ領域、７０８　インターネットに所属するＣＰＵの使用するメモリ領域、７０９　排他制御のために使用する共有メモリ領域、８０１　クライアント側アプリケーションプログラム部、８０２　クライアント側ファイルシステム部、８０３　クライアント側データ暗号／復号化実行部、９０１　代理サーバー、９０２　ＬＡＮ、９０３，９０４　クライアント、１００１　ファイルエントリ、１００２　ユーザーＩＤフィールド、１００３　ファイル名フィールド、１００４　クライアント認証キーフィールド、１００５　ファイルオープン属性フィールド、１００６　ファイルのオープンアカウントフィールド、１００７　先頭セクタの管理テーブルへのポインタフィールド、１００８　ファイルのセクタ番号、１００９　次管理テーブルへのポインタ、１０１０　セクタデータ領域へのポインタ、１０１１　セクタデータ領域、３４０１　新暗号鍵、３６０１　ユーザーＩＤ、３６０２　旧暗号鍵、３６０３　新暗号鍵。

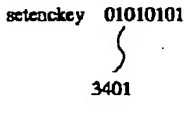
【図３】



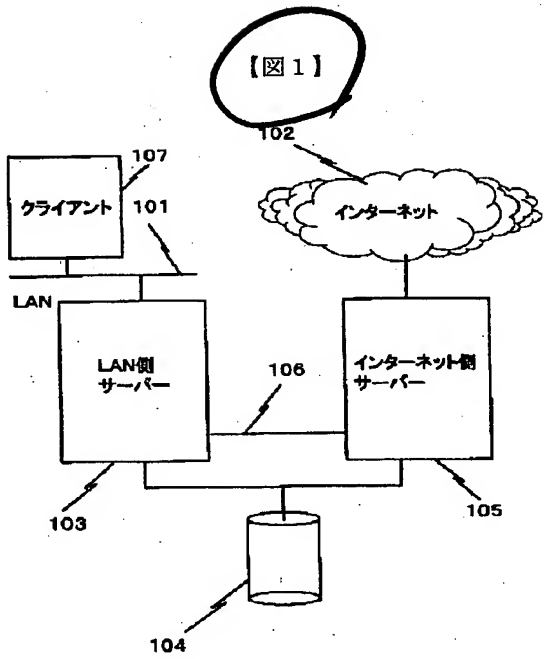
【図１７】



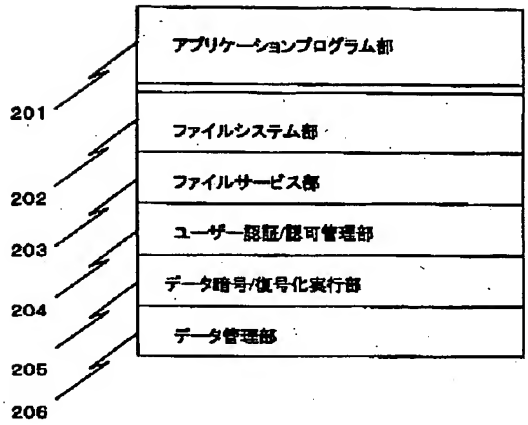
【図３４】



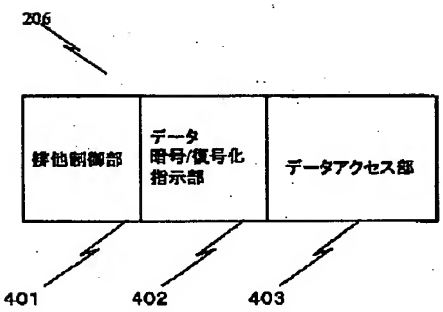
【図１】



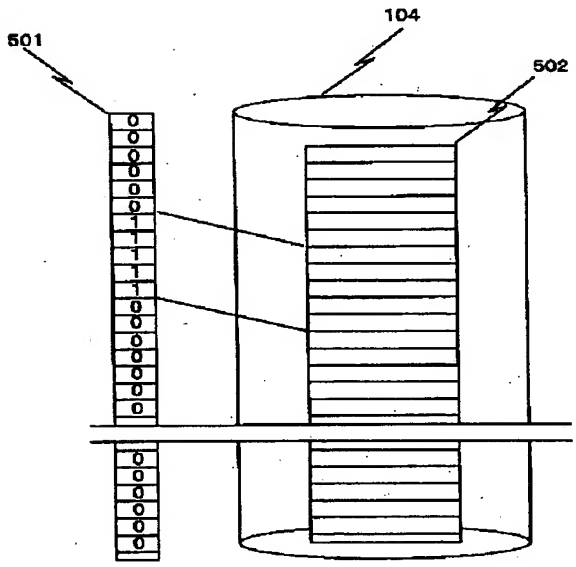
【図２】



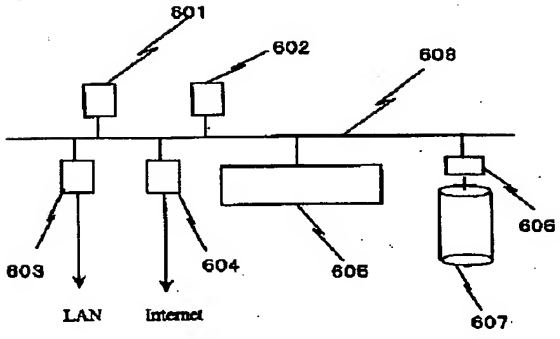
【図４】



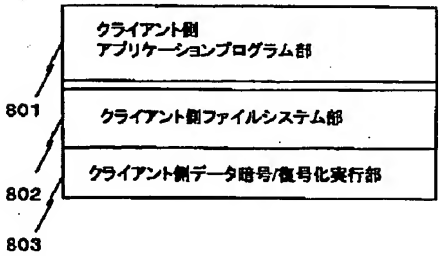
【図５】



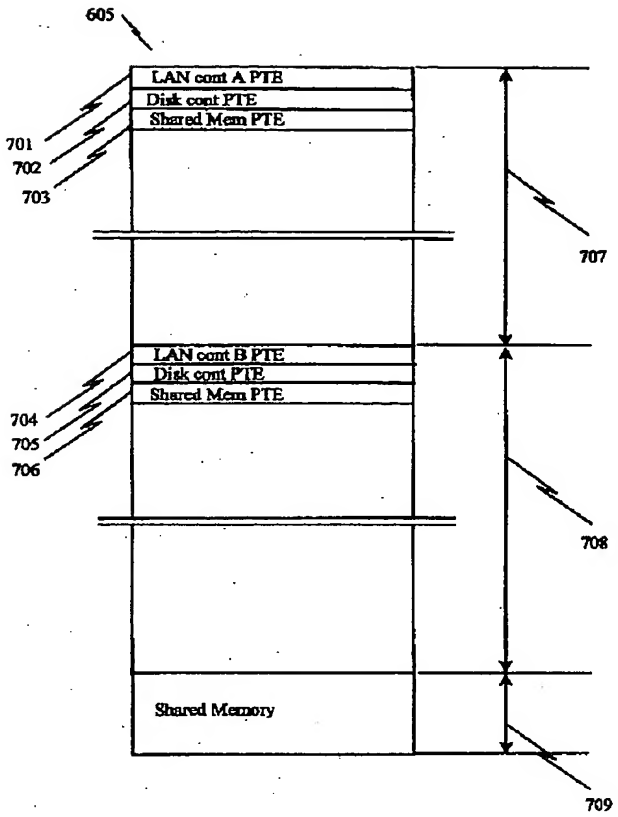
【図６】



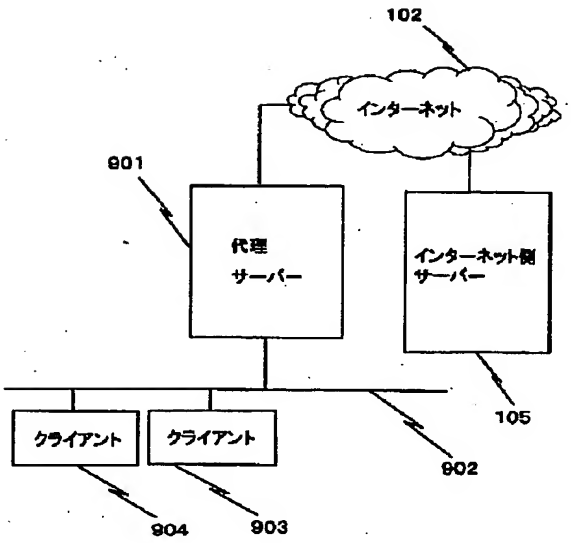
【図８】



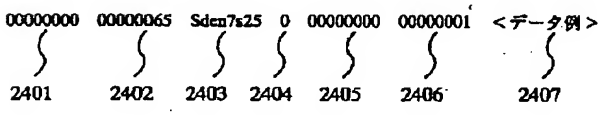
【図７】



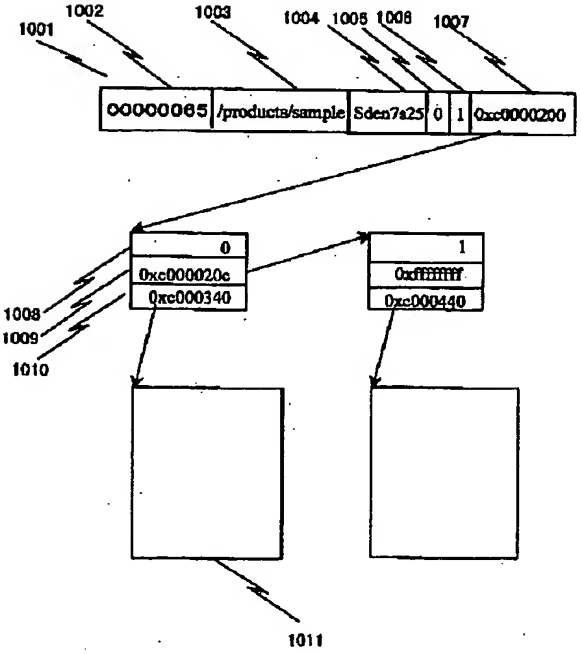
【図９】



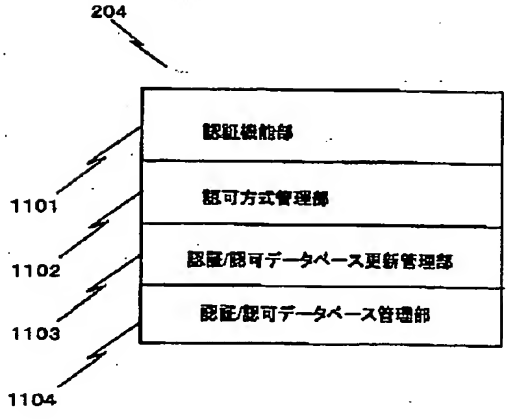
【図２４】



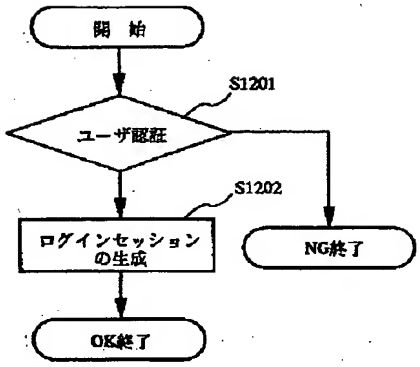
【図１０】



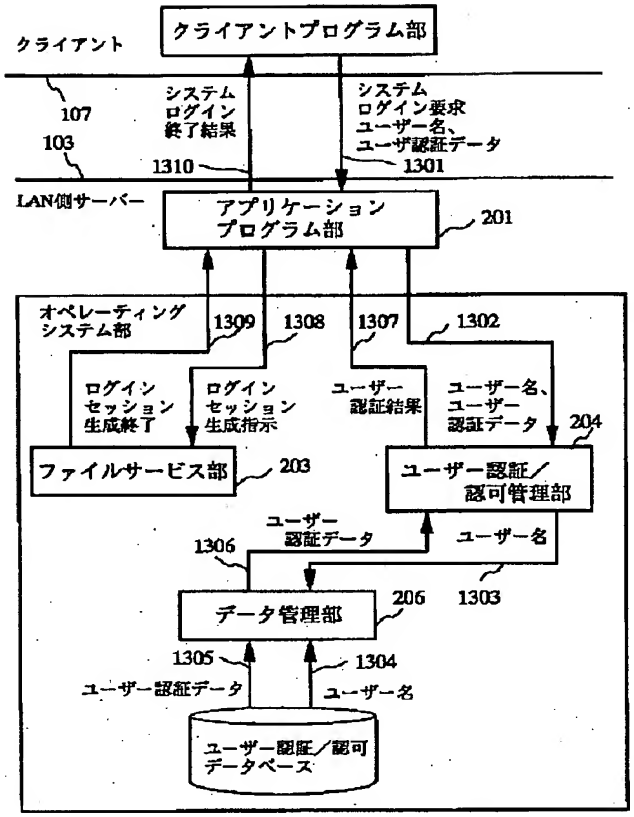
【図１１】



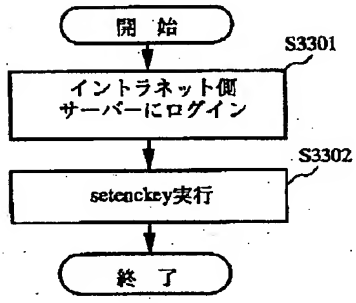
【図１２】



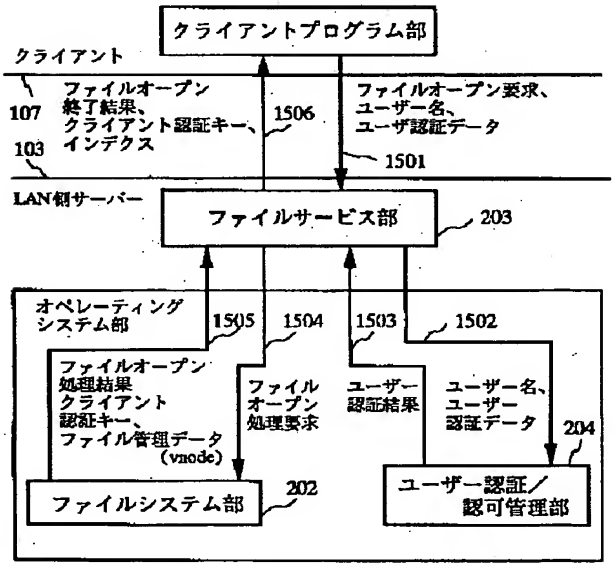
【図１３】



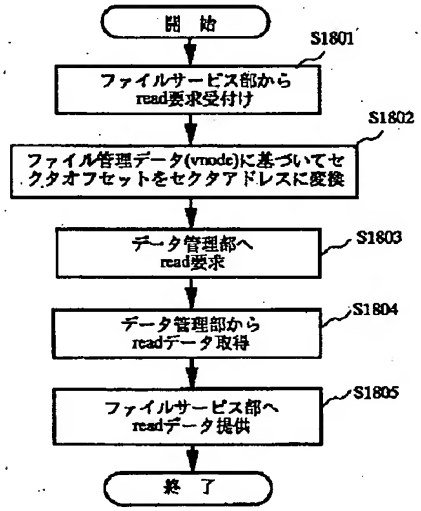
【図３３】



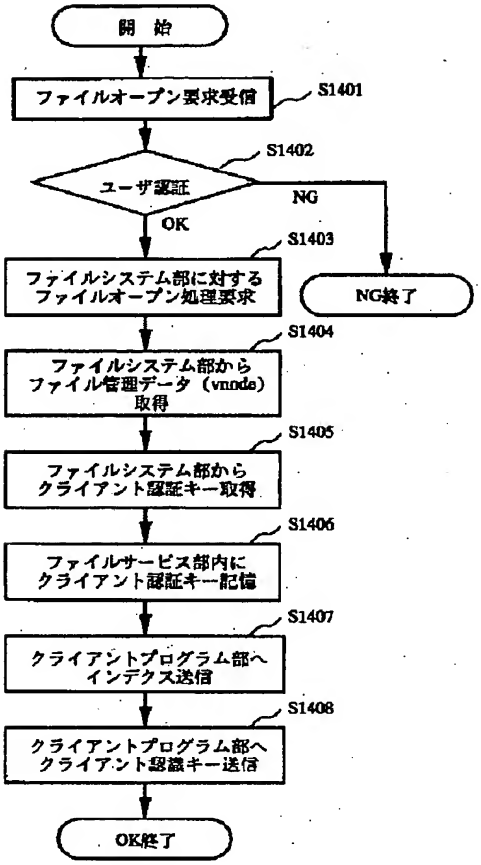
【図１５】



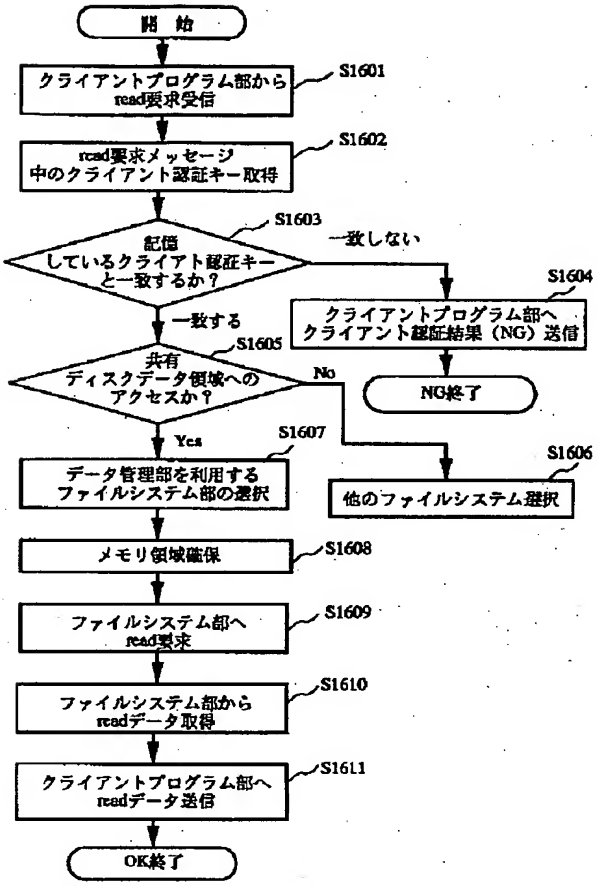
【図１８】



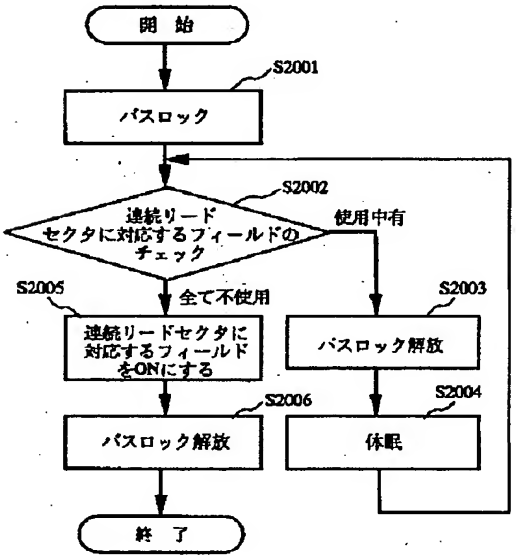
【図１４】



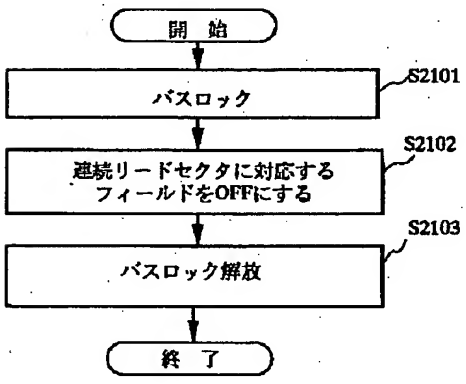
【図１６】



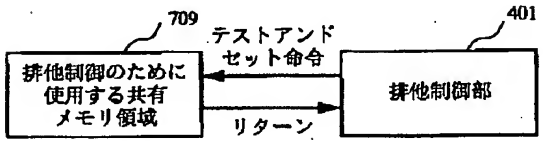
【図２０】



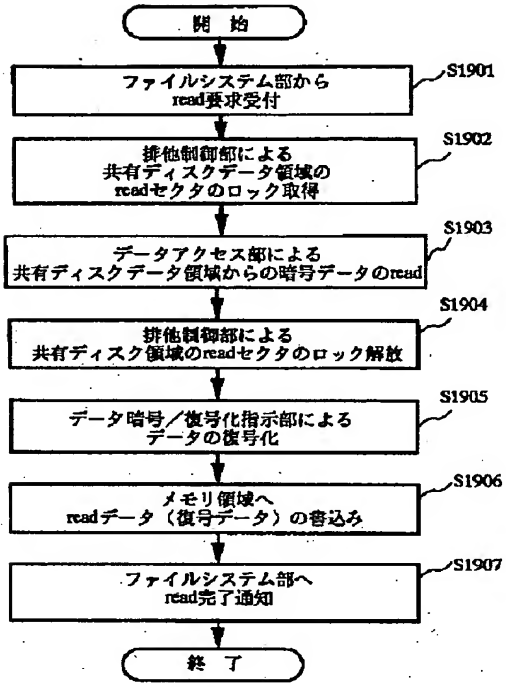
【図２１】



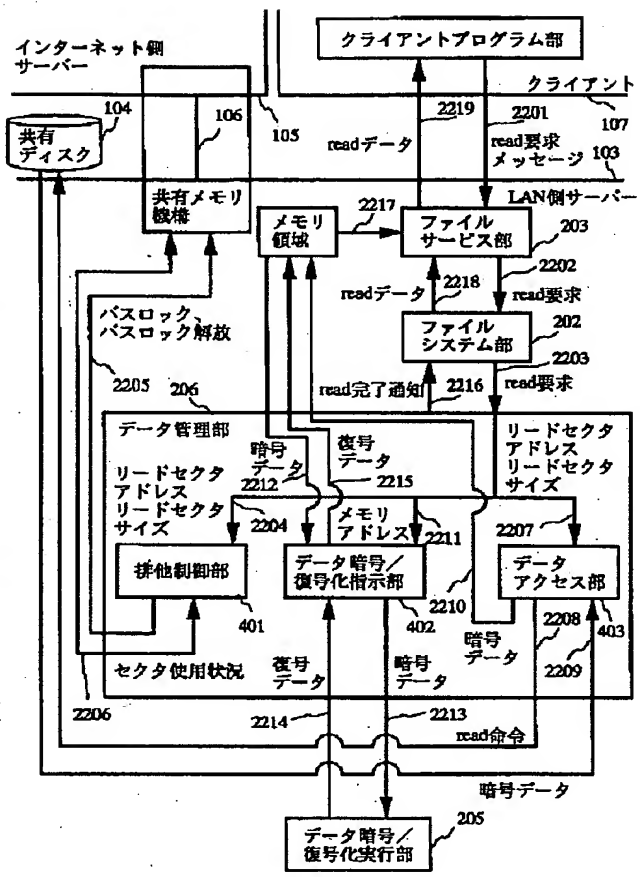
【図３１】



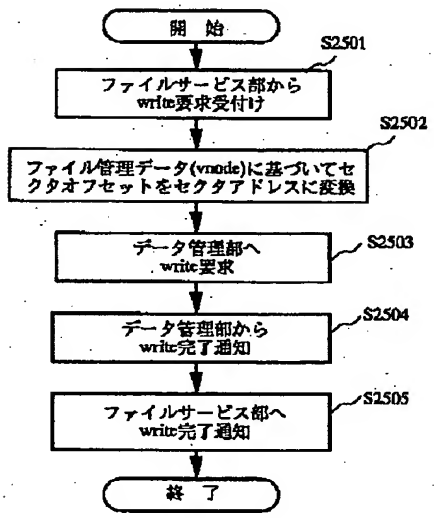
【図１９】



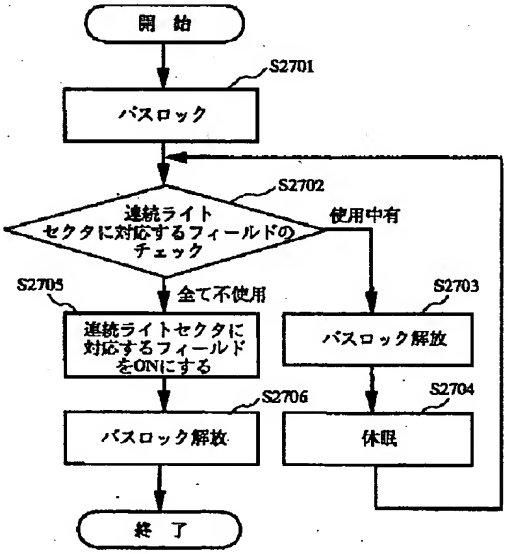
【図２２】



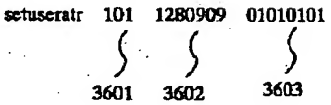
【図２５】



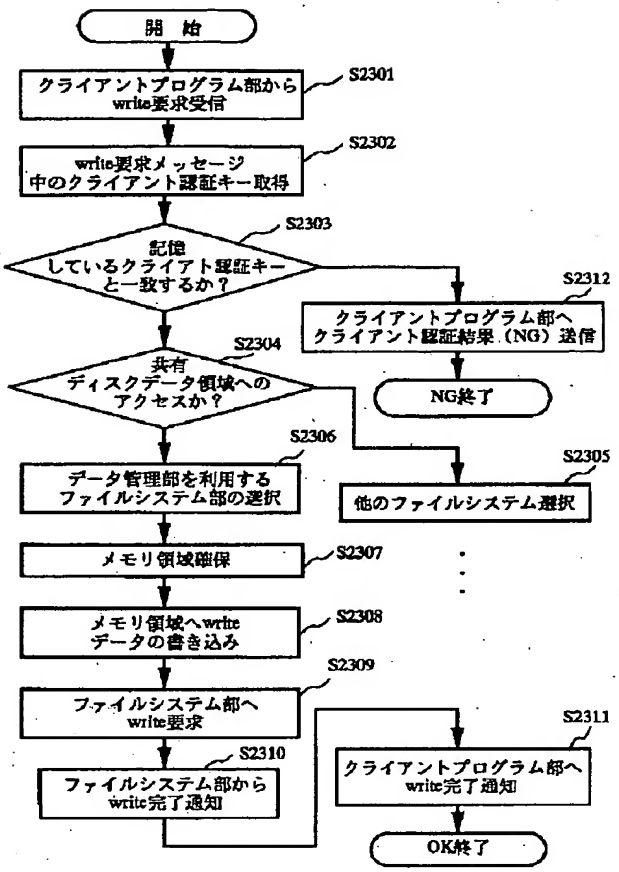
【図２７】



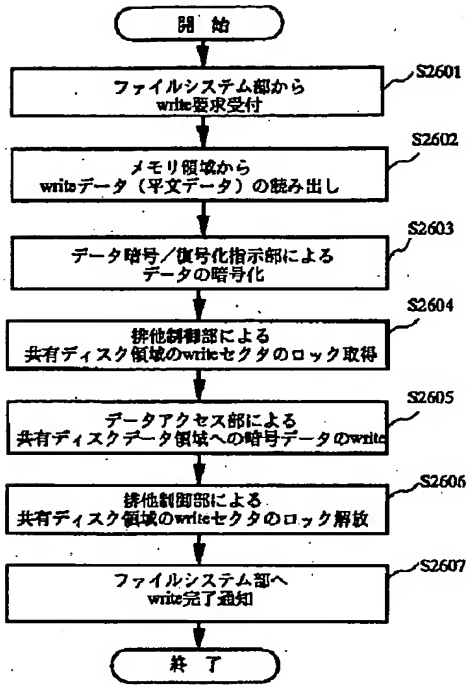
【図３６】



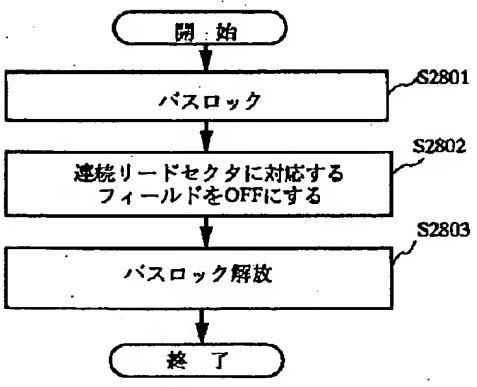
【図２３】



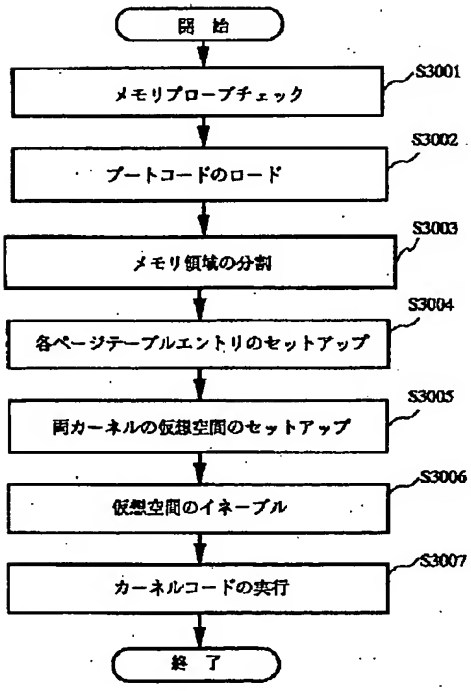
【図２６】



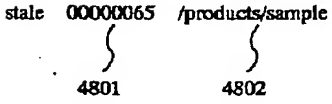
【図２８】



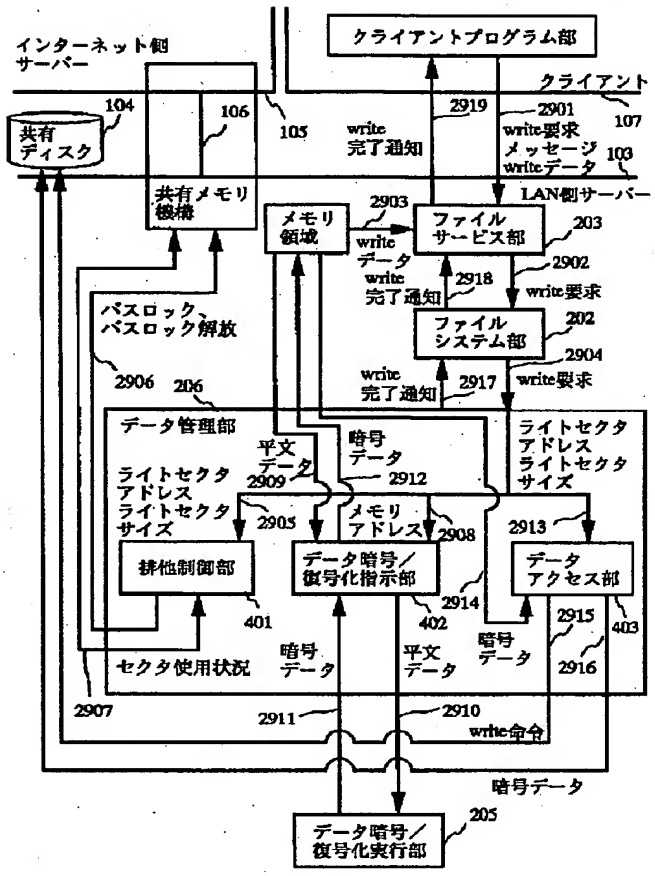
【図３０】



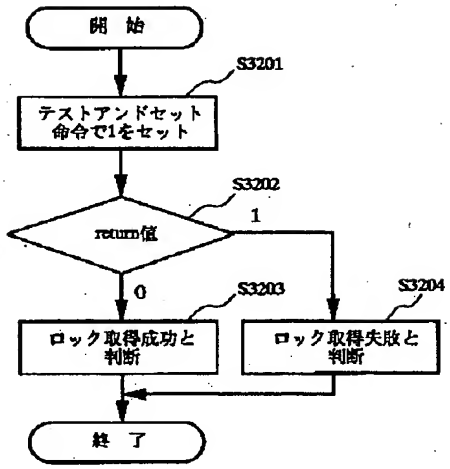
【図４８】



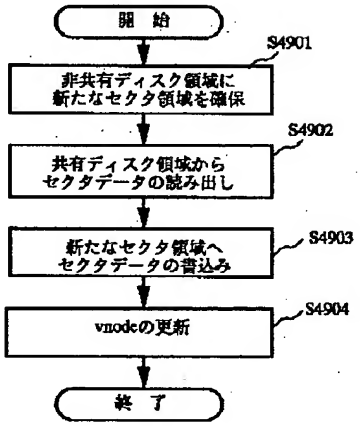
【図２９】



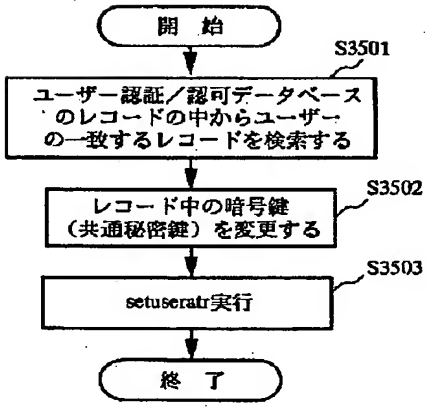
【図３２】



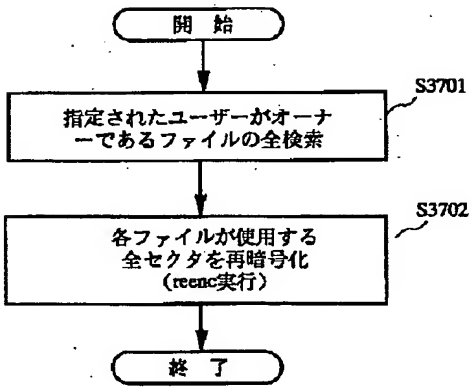
【図４９】



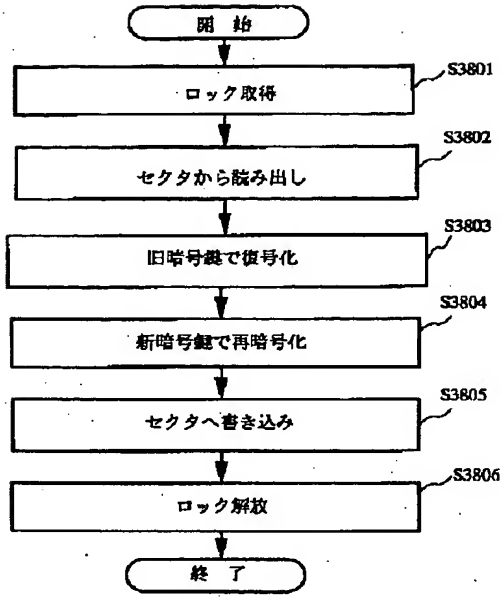
【図３５】



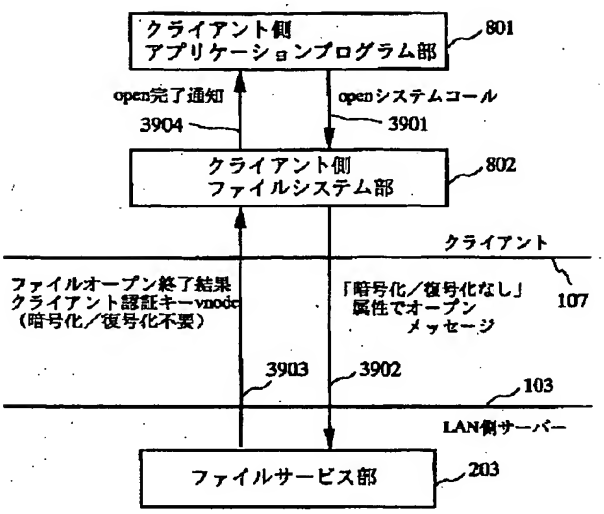
【図３７】



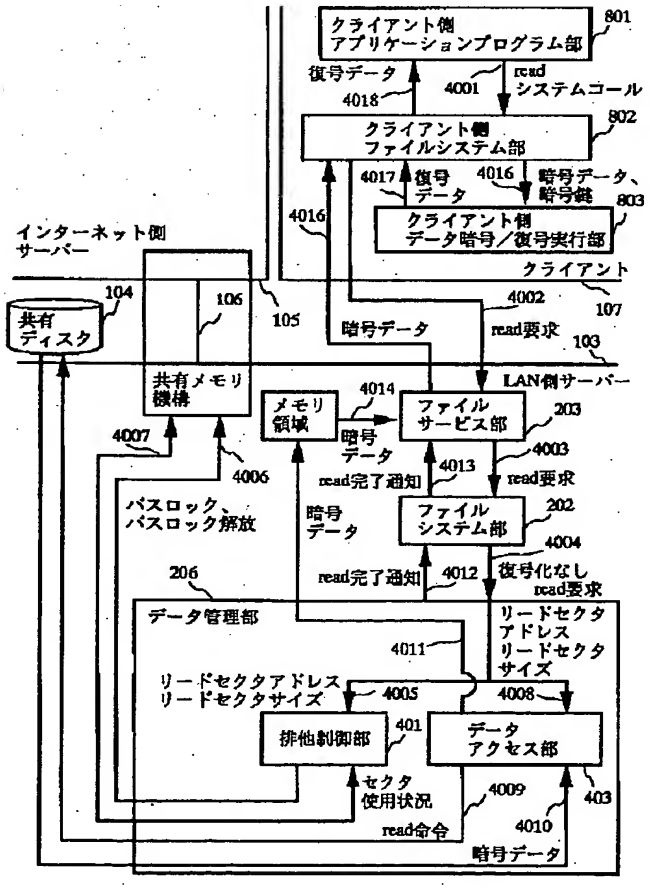
【図３８】



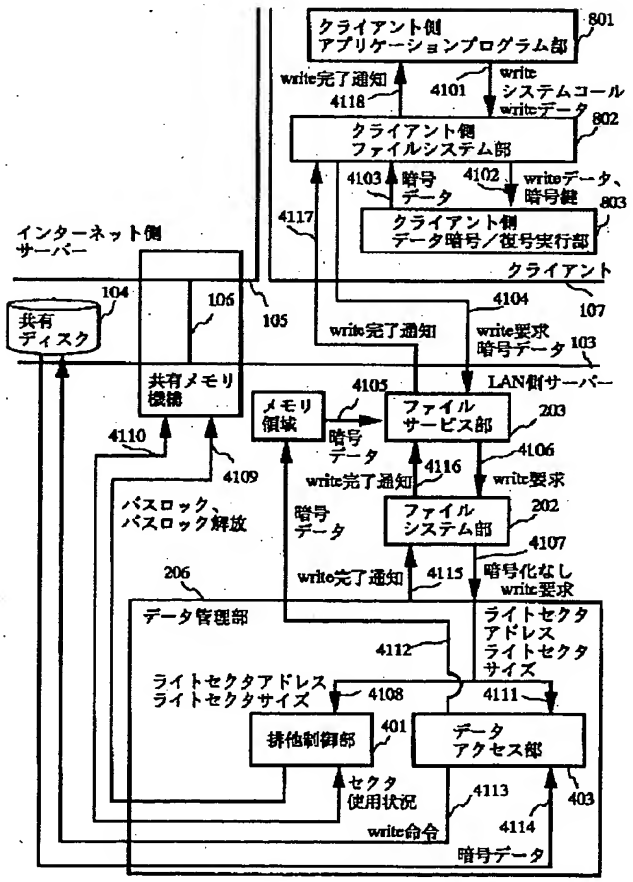
【図３９】



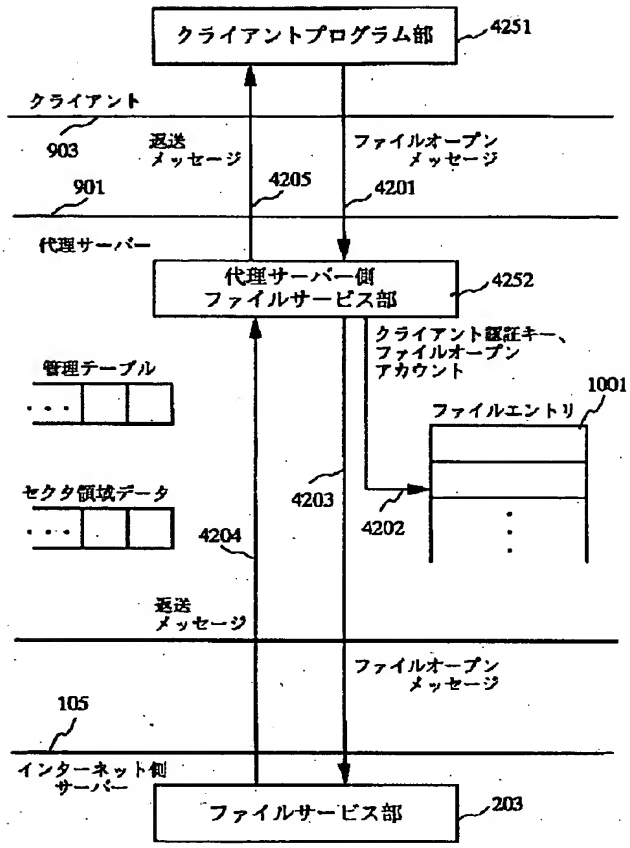
【図４０】



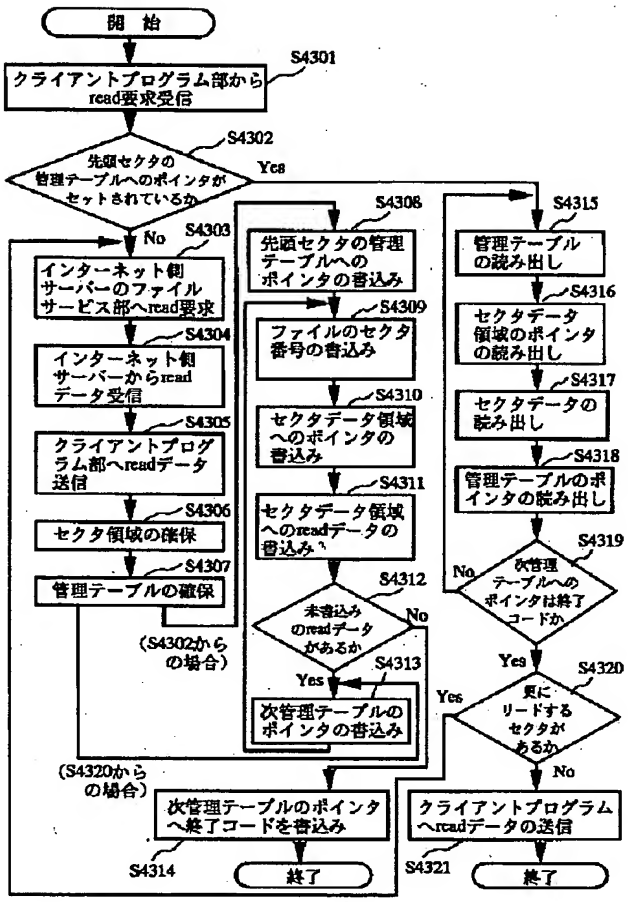
【図４１】



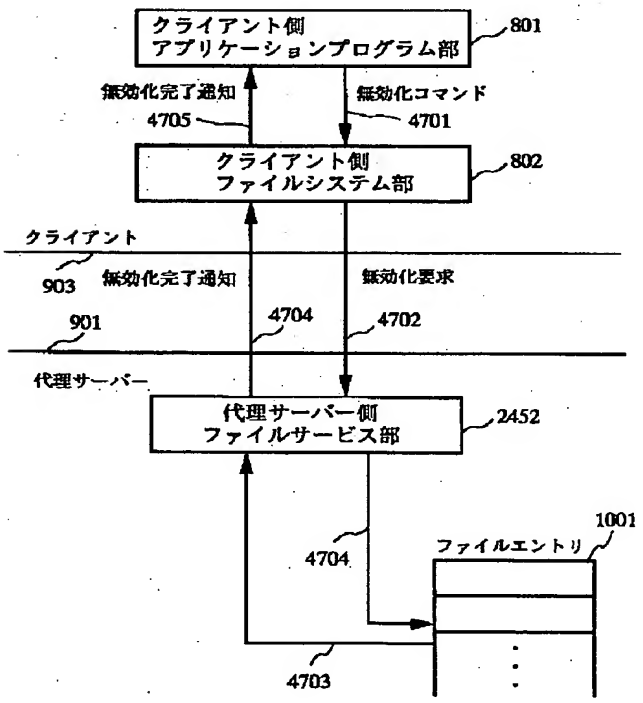
【図４２】


クライアントプログラム部
4251
クライアント
903
返送
メッセージ
ファイルオープン
メッセージ
901
4205
4201
代理サーバー
代理サーバー側
ファイルサービス部
4252
クライアント認証キー、
ファイルオープン
アカウント
管理テーブル
1001
ファイルエントリ
セクタ領域データ
4203
4202
4204
返送
メッセージ
ファイルオープン
メッセージ
105
インターネット側
サーバー
ファイルサービス部
203

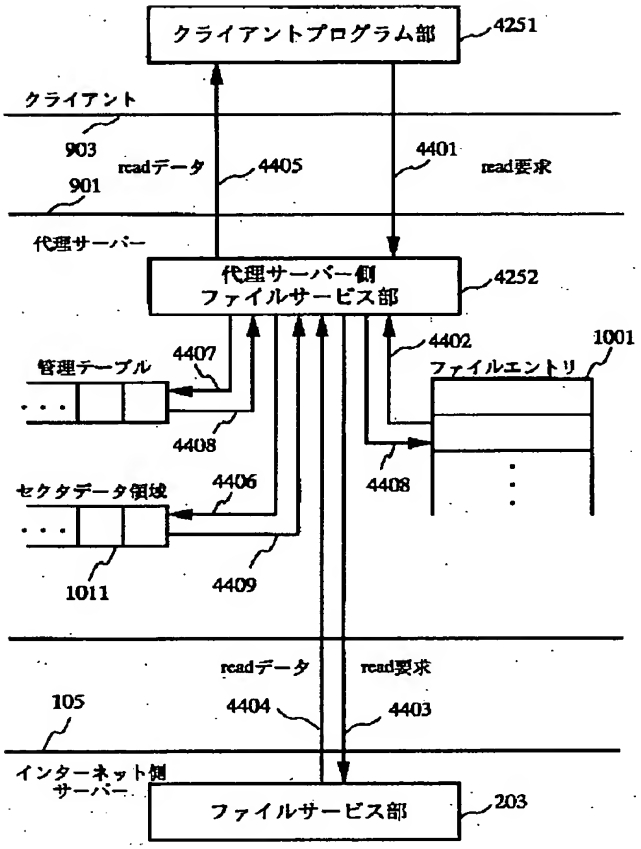
【図４３】


開 始
S4301
クライアントプログラム部から
read要求受信
S4302
先頭セクタの
管理テーブルへのポインタが
セットされているか
Yes
No
S4303
インターネット側
サーバーのファイル
サービス部へread要求
S4304
インターネット側
サーバーからread
データ受信
S4305
クライアントプログ
ラム部へreadデータ
送信
S4306
セクタ領域の確保
S4307
管理テーブルの確保
(S4302から
の場合)
S4308
先頭セクタの管理
テーブルへの
ポインタの書込み
S4309
ファイルのセクタ
番号の書込み
S4310
セクタデータ領域
へのポインタの
書込み
S4311
セクタデータ領域
へのreadデータの
書込み
S4312
未書込み
のreadデータ
があるか
No
Yes
S4313
次管理テーブルの
ポインタの書込み
(S4320から
の場合)
次管理テーブルのポインタ
へ終了コードを書込み
S4314
終了
S4315
管理テーブル
の読み出し
S4316
セクタデータ
領域のポインタ
の読み出し
S4317
セクタデータの
読み出し
S4318
管理テーブルのポ
インタの読み出し
S4319
次管理
テーブルへの
ポインタは終了
コードか
No
Yes
S4320
更に
リードする
セクタが
あるか
Yes
No
クライアントプログラム
へreadデータの送信
S4321
終了

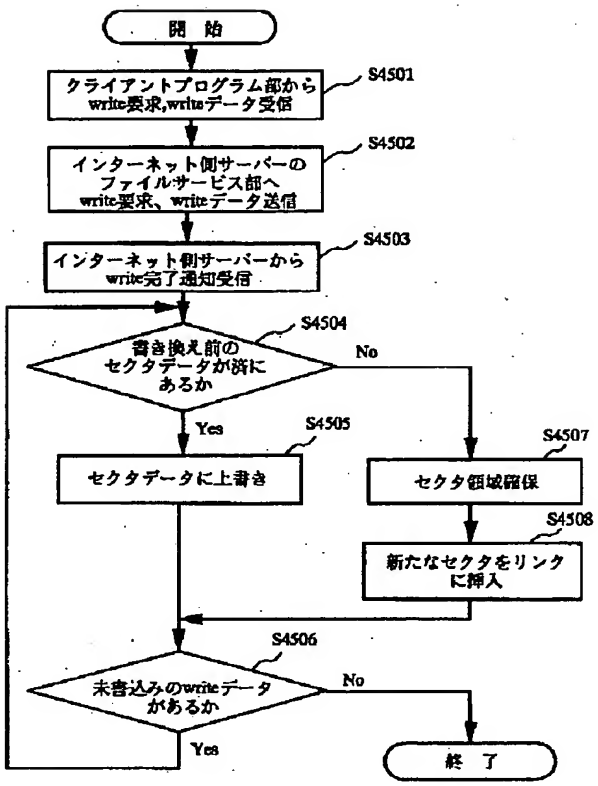
【図４７】


クライアント側
アプリケーションプログラム部
801
無効化完了通知
無効化コマンド
4705
4701
クライアント側
ファイルシステム部
802
クライアント
903
無効化完了通知
無効化要求
901
4704
4702
代理サーバー
代理サーバー側
ファイルサービス部
2452
1001
ファイルエントリ
4704
4703

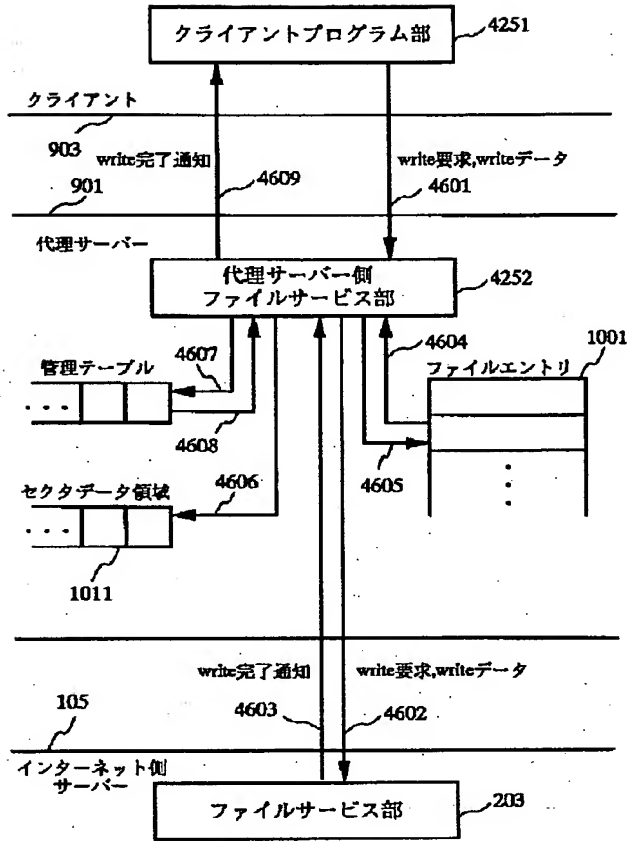
【図４４】


クライアントプログラム部
4251
クライアント
903
901
readデータ
4405
4401
read要求
代理サーバー
代理サーバー側
ファイルサービス部
4252
管理テーブル
4407
4408
4402
ファイルエントリ
1001
4408
セクタデータ領域
4406
1011
4409
readデータ
read要求
105
4404
4403
インターネット側
サーバー
ファイルサービス部
203

【図４５】


開 始
クライアントプログラム部から
write要求,writeデータ受信
S4501
インターネット側サーバーの
ファイルサービス部へ
write要求、writeデータ送信
S4502
インターネット側サーバーから
write完了通知受信
S4503
書き換え前の
セクタデータが済に
あるか
S4504
No
Yes
セクタデータに上書き
S4505
セクタ領域確保
S4507
新たなセクタをリンク
に挿入
S4508
未書込みのwriteデータ
があるか
S4506
No
Yes
終 了

【図４６】


クライアントプログラム部
4251
クライアント
903
write完了通知
4609
write要求,writeデータ
4601
901
代理サーバー
代理サーバー側
ファイルサービス部
4252
4604
1001
管理テーブル
4607
ファイルエントリ
4608
4605
セクタデータ領域
4606
1011
write完了通知
write要求,writeデータ
105
4603
4602
インターネット側
サーバー
ファイルサービス部
203